#2

S&H Form: (2/01)

Attorney Docket No. 1075.1166

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Takashi SHINZAKI

Application No.: Group Art Unit:

Filed: May 22, 2001 Examiner:

For: PUBLICATION CERTIFYING SYSTEM, VIEWING-ACCESS-LOG RECORDING SERVER, PUBLISHING-ACCESS-LOG RECORDING SERVER, DIGITAL-SIGNATURE SERVER, AND INFORMATION TERMINAL FOR ACCESS-TO-VIEW

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-368514

Filed: December 4, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 5/22/01

By: _____
James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年１２月　４日

出願番号
Application Number: 特願２０００－３６８５１４

出願人
Applicant (s): 富士通株式会社

２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０１４９１８

【書類名】　特許願

【整理番号】　0052178

【提出日】　平成12年12月 4日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 19/00

【発明の名称】　公開立証システム並びに閲覧アクセスログ記録サーバ，掲載アクセスログ記録サーバおよびデジタル署名サーバ並びに閲覧アクセス用情報端末

【請求項の数】　5

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　新崎　卓

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100092978

【弁理士】

【氏名又は名称】　真田　有

【電話番号】　0422-21-4222

【手数料の表示】

【予納台帳番号】　007696

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704824

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　公開立証システム並びに閲覧アクセスログ記録サーバ，掲載アクセスログ記録サーバおよびデジタル署名サーバ並びに閲覧アクセス用情報端末

【特許請求の範囲】

【請求項１】　提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとをそなえたことを特徴とする、公開立証システム。

【請求項２】　通信ネットワークを介して閲覧された公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有することを特徴とする、閲覧アクセスログ記録サーバ。

【請求項３】　通信ネットワークを介して情報提供サーバに送信・掲載された公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有することを特徴とする、掲載アクセスログ記録サーバ。

【請求項４】　提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開

情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成するデジタル署名サーバであって、

該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、該デジタル署名サーバの秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能とを有することを特徴とする、デジタル署名サーバ。

【請求項５】　提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成する情報端末であって、

該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なうことを特徴とする、閲覧アクセス用情報端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子データが通信ネットワーク上で第三者が閲覧・アクセス可能な状態で保管されていたこと、即ち、電子データが通信ネットワーク上で第三者に対して公開されていたことを立証するための、公開立証システム並びに閲覧アクセスログ記録サーバ，掲載アクセスログ記録サーバおよびデジタル署名サーバ並びに閲覧アクセス用情報端末に関し、例えば、企業からの各種情報（例えばリコ

ールに伴う製品障害情報，製品回収情報等）が電子データとして通信ネットワーク上で掲示・公開されていたことや、各種技術情報が電子データとして通信ネットワーク上で公開されて公知化されていることを証明する手段（サービス）として広く活用されうるものである。

【０００２】

【従来の技術】

近年、紙等の印刷物によって情報の開示を行なう代わりに、その情報をインターネット〔例えばＷＷＷ（World Wide Web）〕上で電子データとして掲示・公開することが一般的になっている。

より具体的に説明すると、情報掲載希望者は、例えばパソコン等の情報端末からインターネットを介して情報提供サーバにアクセスし、掲載希望情報を情報提供サーバに送信し、その情報を情報提供において電子データとして外部からアクセス可能な状態で保管させる。これにより、第三者は、パソコン等の情報端末からインターネットを介して情報提供サーバにアクセスすれば、その情報提供サーバに保管された電子データを閲覧することができるようになっている。

【０００３】

【発明が解決しようとする課題】

ところで、近年、電子データがいつ作成されたかを立証するために、公開鍵暗号化技術やメッセージダイジェスト作成技術を組み合わせたデジタル署名技術が用いられ始めている。

しかし、特許審査等に際しての公知例範囲にインターネット上での公開情報を含める場合や、企業がＷＷＷ上で例えばリコールに伴う製品障害情報，製品回収情報等の告知を行なう場合、その情報としての電子データの作成日時を立証するだけでなく、その電子データが第三者からのアクセスが容易な場所（サーバ）で掲示・公開されていたことや、その電子データが掲示・公開されていた期間を立証することが必要になる。

【０００４】

例えば、雑誌等については国立国会図書館でそのほとんどを保管されているため、その情報の公開を立証することが比較的容易であるが、電子データが通信ネ

ットワーク上において第三者が閲覧可能な状態で掲示・公開されていた日時（期間）を立証することには困難が伴っている。このため、現状では、電子データの通信ネットワーク上での公開を立証するための手法やシステムは確立されておらず、その手法やシステムの開発が強く望まれている。

【０００５】

本発明は、このような要望に鑑み創案されたもので、各種情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証できるようにして、その通信ネットワーク上で掲示・公開された情報にも、印刷物や出版物と同様の証拠能力をもたせることを実現した、公開立証システム並びに閲覧アクセスログ記録サーバ，掲載アクセスログ記録サーバおよびデジタル署名サーバ並びに閲覧アクセス用情報端末を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上記目的を達成するために、本発明の公開立証システム（請求項１）は、提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとをそなえたことを特徴としている。

【０００７】

また、本発明の閲覧アクセスログ記録サーバ（請求項２）は、通信ネットワークを介して閲覧された公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有することを特徴としている。

【０００８】

上述の構成により、第三者が、情報提供サーバに保存されている公開情報を閲覧すべく、情報端末から通信ネットワークを介して公開情報にアクセスすると、その公開情報は、公開情報掲示機能により第三者に提供される。その際、閲覧アクセスログ記録サーバにおいて、第三者によって閲覧された公開情報とその公開情報に対するアクセス日時とが閲覧アクセスログとして獲得され保存される。

【０００９】

このようにして、第三者により閲覧された公開情報について、その内容と閲覧日時とが閲覧アクセスログとして記録されることになる。従って、この閲覧アクセスログにより、少なくともその閲覧日時には、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。

【００１０】

本発明の掲載アクセスログ記録サーバ（請求項３）は、通信ネットワークを介して情報提供サーバに送信・掲載された公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有することを特徴としている。

【００１１】

上述の構成により、公開情報の掲載希望者が、その公開情報を、通信ネットワークを介して情報提供サーバに送信して掲載する際、掲載アクセスログ記録サーバにおいて、掲載希望者によって掲載された公開情報とその公開情報の掲載日時とが掲載アクセスログとして記録されることになる。従って、この掲載アクセスログにより、その掲載日時以降、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。

【００１２】

さらに、本発明のデジタル署名サーバ（請求項４）は、上述した情報提供サー

バおよび閲覧アクセスログ記録サーバとともに、公開立証システムを構成するものであって、該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、該デジタル署名サーバの秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能とを有することを特徴としている。

【００１３】

上述の構成により、閲覧アクセスログ記録サーバで得られた閲覧アクセスログにタイムスタンプを付加した状態で、デジタル署名サーバの秘密鍵を用いてデジタル署名が施される。このデジタル署名サーバを第三者である電子公証会社等のものとすることで、閲覧アクセスログの証拠能力を高めることができる。

【００１４】

そして、本発明の閲覧アクセス用情報端末（請求項５）は、上述した情報提供サーバおよび閲覧アクセスログ記録サーバとともに、公開立証システムを構成するものであって、該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なうことを特徴としている。

【００１５】

このような閲覧アクセス用情報端末により、閲覧アクセスログ記録サーバにおいて公開情報に対する閲覧アクセスログが定期的に且つ自動的に記録・保存される。従って、この閲覧アクセスログにより、少なくとも、この閲覧アクセス用情報端末が定期的な閲覧アクセスを行なっていた期間については、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。

【００１６】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態を説明する。

〔１〕第１実施形態の説明

図１は本発明の第１実施形態としての公開立証システムの構成を示すブロック

図であり、この図１に示すように、第１実施形態の公開立証システム１Ａは、情報提供サーバ１０と公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ）２０Ａとをそなえて構成されている。

【００１７】

情報提供サーバ１０は、通信ネットワーク２を介して、情報端末３０に対し公開情報の提供を行なうもので、後述するデータ送受信機能１１，公開情報保存機能１２および公開情報掲示機能１３を有している。なお、本実施形態では、通信ネットワーク２が、インターネット上に構築されたWWW（World Wide Web）である場合について説明する。

【００１８】

また、公開情報アクセスログ記録サーバ２０Ａは、通信ネットワーク２上において情報提供サーバ１０と情報端末３０との間に配置され、情報端末３０による情報提供サーバ１０（公開情報）に対するアクセスログを記録すべく、後述するデータ送受信機能２１，データトラップ機能２２およびデータ保存機能２３を有している。本実施形態において、情報提供サーバ１０と情報端末３０との間で送受信されるデータ群は、公開情報アクセスログ記録サーバ２０Ａを経由・通過するようになっている。

【００１９】

情報提供サーバ１０において、データ送受信機能１１は、通信ネットワーク２を介し、公開情報アクセスログ記録サーバ２０Ａへ情報を送信したり公開情報アクセスログ記録サーバ２０Ａから情報を受信したりするためのものである。

また、公開情報保存機能１２は、提供すべき公開情報を電子データとして保存するためのものである。

【００２０】

さらに、公開情報掲示機能１３は、公開情報を閲覧すべく通信ネットワーク２を介してアクセスしてきた情報端末３０に対しその公開情報を提供するために、その公開情報（電子データ）を、公開情報保存機能１２から読み出して、データ送受信機能１１，通信ネットワーク２および公開情報アクセスログ記録サーバ２０Ａを通じて情報端末３０に返送するものである。

【００２１】

一方、公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ）２０Ａにおいて、データ送受信機能２１は、通信ネットワーク２を介し、情報提供サーバ１０や情報端末３０へ情報を送信したり情報提供サーバ１０や情報端末３０から情報を受信したりするためのものである。

また、データトラップ機能（閲覧アクセスログ獲得機能）２２は、情報端末３０により通信ネットワーク２を介して閲覧された公開情報と、その公開情報に対するアクセス日時を含む、情報端末３０のアクセスログとを閲覧アクセスログ（公開情報アクセスログ，閲覧アクセス記録証拠データ群）として獲得するものである。

【００２２】

つまり、データトラップ機能２２は、情報端末３０から情報提供サーバ１０に対する閲覧アクセスが行なわれた場合、情報端末３０と情報提供サーバ１０との間で通信ネットワーク２を介してやり取りされるデータ群（公開情報アクセスログ記録サーバ２０Ａを経由・通過するデータ群）から、上述した各種データを閲覧アクセスログとしてトラップするものである。

【００２３】

なお、ここでは、データトラップ機能２２が、閲覧された公開情報と情報端末３０のアクセスログとの両方を獲得するものとしているが、このデータトラップ機能２２を、公開情報とアクセスログとをそれぞれ獲得する別々の機能（例えば閲覧データトラップ機能とアクセスログ機能と）に分離してもよい。

【００２４】

図２は、本実施形態において獲得・保存されるアクセスログの例を説明するための図であり、この図２に示すように、アクセスログとしては、アクセス年月日およびアクセス時刻のほかに、ドメイン情報，リモートホスト情報，ブラウザ名称情報や参照ディレクトリ情報などが含まれる。また、アクセスログは上述したものに限られず、公開情報にアクセスした情報端末（アクセス元）３０にかかる端末情報、例えば、閲覧者（情報端末３０）側の通信ネットワークアドレス，氏名，アクセス経路などをアクセスログとしてさらに獲得してもよい。

【００２５】

さらに、データ保存機能（閲覧アクセスログ保存機能）２３は、データトラップ機能２２によってトラップされた、公開情報データとアクセスログとをペアにし、閲覧アクセスログ（公開情報アクセスログ，閲覧アクセス記録証拠データ群）として保存するためのものである。

なお、情報端末３０は、上述したように情報提供サーバ１０における公開情報を検索・閲覧するために用いられるもので、例えばパーソナルコンピュータや携帯電話等の情報端末機器であり、データ送受信機能３１およびWWWブラウザ３２を有している。

【００２６】

ここで、データ送受信機能３１は、通信ネットワーク２を介し、公開情報アクセスログ記録サーバ２０Ａへ情報を送信したり公開情報アクセスログ記録サーバ２０Ａから情報を受信したりするためのものである。WWWブラウザ（インターネットブラウザソフトウェア）３２は、通信ネットワーク２を介して即ちWWWにより、情報提供サーバ１０に対する閲覧アクセス等を行なう際に用いられるものである。

【００２７】

また、情報提供サーバ１０は例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能１１，公開情報保存機能１２および公開情報掲示機能１３は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

同様に、公開情報アクセスログ記録サーバ２０Ａも例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能２１，データトラップ機能２２およびデータ保存機能２３は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【００２８】

次に、上述のごとく構成された第１実施形態の公開立証システム１Ａおよび公開情報アクセスログ記録サーバ２０Ａの動作について、図３に示すフローチャート（ステップＳ１１～Ｓ１６）に従って説明する。

情報提供サーバ１０における公開情報の閲覧を希望する者（閲覧者，第三者）は、情報端末３０（WWWブラウザ３２）を起動して通信ネットワーク２に接続し、情報提供サーバ１０に対する閲覧アクセスを、通信ネットワーク２を介して行なう（ステップＳ１１）。

【００２９】

そして、情報端末３０は、まず、公開情報アクセスログ記録サーバ２０Ａにアクセスしてから（ステップＳ１２）、情報提供サーバ１０にアクセスし（ステップＳ１３）、情報提供サーバ１０における公開情報を閲覧することが可能な状態となる。

情報提供サーバ１０では、公開情報掲示機能１３により、情報端末３０からの指示に応じて、閲覧者の望む公開情報が、公開情報保存機能１２から検索されて読み出され、公開情報アクセスログ記録サーバ２０Ａを経由して情報端末３０に返送され、閲覧者に提供される（ステップＳ１４）。

【００３０】

公開情報が公開情報アクセスログ記録サーバ２０Ａを経由する際、公開情報アクセスログ記録サーバ２０Ａにおいては、データトラップ機能２２により、閲覧者（第三者）が閲覧した公開情報と、その公開情報に対するアクセス日時を含む情報端末３０のアクセスログとが、閲覧アクセスログとしてトラップされ（ステップＳ１５）、データ保存機能２３によって保存される（ステップＳ１６）。

【００３１】

上述のごとく、公開立証システム１Ａは、閲覧者側の情報端末３０から情報提供サーバ１０上の公開情報をアクセスする場合、公開情報アクセスログ記録サーバ２０Ａを経由してアクセスする仕組みとなっている。そして、公開情報アクセスログ記録サーバ２０Ａでは、情報端末３０からアクセス・閲覧された公開情報の内容データとアクセス日時等を含むアクセスログとが、閲覧アクセスログとして保存される。アクセスログとしては、アクセス日時のみに限らず、閲覧者側の通信ネットワークアドレス，氏名，アクセス経路等の端末情報をトラップして保存する。このようにして閲覧された公開情報データとアクセスログとをペアにして保存することで、前記公開情報データが公開情報としてアクセス可能であった

という証拠を残すことが可能になる。

【００３２】

このように、本発明の第１実施形態としての公開立証システム１Ａや公開情報アクセスログ記録サーバ２０Ａによれば、第三者である閲覧者により閲覧された公開情報について、その内容と閲覧日時とが閲覧アクセスログとして記録され、公開情報の公開履歴を、閲覧アクセスログにより証明可能な形式で保存することができるので、少なくともその閲覧日時には、その公開情報が電子データとして通信ネットワーク２上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク２上で掲示・公開されていたことを立証することができる。従って、情報提供サーバ１０により通信ネットワーク２上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる。

【００３３】

また、第１実施形態の公開立証システム１Ａや公開情報アクセスログ記録サーバ２０Ａを用いることにより、電子公証だけでなく、情報開示の開示記録や、アクセスが可能であったことの証明を行なうサービスを提供することができ、新規ビジネス創出の可能性が大きく広がる。

【００３４】

さらに、閲覧アクセスログとして、公開情報にアクセスした情報端末３０にかかる端末情報（通信ネットワークアドレス，氏名，アクセス経路など）を獲得し保存することにより、閲覧アクセスログに含まれる端末情報に基づいて、どの情報端末３０がどのような経路で公開情報に対して閲覧アクセスを行なったかを特定することが可能になり、閲覧アクセスログの証拠能力をより高めることができる。

【００３５】

またさらに、本実施形態の公開立証システム１Ａを用いて、電子データが通信ネットワーク２上で第三者が閲覧可能な状態で公開されていた日時を立証するサービスを提供することにより、様々な局面で電子データを証拠として使用することが可能になる。

例えば、ＰＬ（Product Liability）法の立場から言えば、企業側が、製品の

問題情報や回収情報をＷｅｂ（通信ネットワーク２）上に公開し閲覧可能な状況にしていた期間を証明することが可能になり、企業側が通知義務に対して努力をしていたことを証明できる。

【００３６】

逆に、消費者側は、本サービスを利用することで、企業が、ある特定ページを公開していたという事実を第三者デジタル署名を行なって記録保存することにより、誇大広告や契約違反の証拠を残すことも可能になる。つまり、情報提供サーバ１０の管理者側が本サービスを使用するのではなく、情報アクセス側が本サービスを利用するのである。また、Ｗｅｂ（通信ネットワーク２）上での公開掲示板に誹謗中傷の文書が記載された場合にも本公開立証システム１Ａを使用することにより名誉毀損の証拠を確実に残すことが可能になる。

【００３７】

なお、上述した第１実施形態では、便宜上、情報提供サーバ１０と公開情報アクセスログ記録サーバ２０Ａとを分けて説明したが、情報提供サーバ１０としての機能と公開情報アクセスログ記録サーバ２０Ａとしての機能との両方を、物理的に一つのサーバマシンの中に組み込むことも可能である。ここで言うサーバとは、機能としてのサーバである。このように一つのサーバを、情報提供サーバ１０および公開情報アクセスログ記録サーバ２０Ａとして兼用することにより、２種類のサーバを別々にそなえる必要がなくなり、公開立証システム１Ａをより簡素に構成することができる。

【００３８】

また、公開情報アクセスログ記録サーバ２０Ａとしての機能をインターネットサービスプロバイダのプロキシサーバ内に組み込んでもよい。この場合、情報端末３０において一般に用いられるＷＷＷブラウザ（インタネットブラウザソフトウェア）３２によって指定されるプロキシサーバを、公開情報アクセスログ記録サーバ２０Ａとしての機能を有するプロキシサーバに変更するだけで、情報端末３０は、公開立証システム１Ａを容易に利用することができるほか、インターネットサービスプロバイダが新しいサービスを容易に提供することも可能になる。

【００３９】

さらに、公開情報アクセスログ記録サーバ２０Ａのデータ保存機能２３が、閲覧アクセスログに含まれる公開情報データを圧縮した形で保存してもよい。ハードディスク等の記憶容量を考えると、アクセスログと一緒に保存される、閲覧された公開情報データについては、そのまま保存するよりも、圧縮して保存する方が望ましい。このような圧縮を行なうことにより、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

【００４０】

〔２〕第２実施形態の説明

図４は本発明の第２実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００４１】

図４に示すように、第２実施形態の公開立証システム１Ｂも、第１実施形態の公開立証システム１Ａとほぼ同様に構成されているが、第２実施形態の公開立証システム１Ｂでは、第１実施形態の公開情報アクセスログ記録サーバ２０Ａに代えて公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ）２０Ｂがそなえられている。この公開情報アクセスログ記録サーバ２０Ｂは、第１実施形態と同様のデータ送受信機能２１，データトラップ機能２２およびデータ保存機能２３のほかに、メッセージダイジェスト生成機能２４をさらに有している。

【００４２】

メッセージダイジェスト生成機能２４は、データトラップ機能２２によりトラップされた公開情報のメッセージダイジェストを生成するものであり、この第２実施形態のデータ保存機能２３においては、公開情報そのものに代えて、メッセージダイジェスト生成機能２４により公開情報（閲覧情報）の内容データから生成されたメッセージダイジェストが閲覧アクセスログとして保存されるようになっている。

【００４３】

なお、メッセージダイジェストを作成するには、例えばＭＤ５（Message Digest algorithm 5）等のアルゴリズムが使用される。また、メッセージダイジェス

ト生成機能２４により、閲覧アクセスログの全てについてのメッセージダイジェストを生成してデータ保存機能２３に保存するように構成してもよい。即ち、情報端末３０のアクセスログについてのメッセージダイジェストも生成し、第２実施形態のデータ保存機能２３において、情報端末３０のアクセスログそのものに代え、メッセージダイジェスト生成機能２４によりアクセスログから生成されたメッセージダイジェストを保存してもよい。

【００４４】

また、公開情報アクセスログ記録サーバ２０Ｂも、第１実施形態の公開情報アクセスログ記録サーバ２０Ａと同様、例えばパーソナルコンピュータ等の計算機により構成されており、データ送受信機能２１，データトラップ機能２２，データ保存機能２３およびメッセージダイジェスト生成機能２４は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【００４５】

次に、上述のごとく構成された第２実施形態の公開立証システム１Ｂおよび公開情報アクセスログ記録サーバ２０Ｂの動作について、図５に示すフローチャート（ステップＳ２１～Ｓ２７）に従って説明する。

情報提供サーバ１０における公開情報の閲覧を希望する者（閲覧者，第三者）は、第１実施形態と同様、情報端末３０（ＷＷＷブラウザ３２）を起動して通信ネットワーク２に接続し、情報提供サーバ１０に対する閲覧アクセスを、通信ネットワーク２を介して行なう（ステップＳ２１）。

【００４６】

そして、情報端末３０は、まず、公開情報アクセスログ記録サーバ２０Ｂにアクセスしてから（ステップＳ２２）、情報提供サーバ１０にアクセスし（ステップＳ２３）、情報提供サーバ１０における公開情報を閲覧することが可能な状態となる。

情報提供サーバ１０では、公開情報掲示機能１３により、情報端末３０からの指示に応じて、閲覧者の望む公開情報が、公開情報保存機能１２から検索されて読み出され、公開情報アクセスログ記録サーバ２０Ｂを経由して情報端末３０に返送され、閲覧者に提供される（ステップＳ２４）。

【００４７】

公開情報が公開情報アクセスログ記録サーバ２０Ｂを経由する際、公開情報アクセスログ記録サーバ２０Ｂにおいては、データトラップ機能２２により、閲覧者（第三者）が閲覧した公開情報と、その公開情報に対するアクセス日時を含む情報端末３０のアクセスログとが、閲覧アクセスログとしてトラップされる（ステップＳ２５）。

【００４８】

そして、第２実施形態においては、データトラップ機能２２によりトラップされた公開情報データのメッセージダイジェストが、メッセージダイジェスト生成機能２４により作成され（ステップＳ２６）、このメッセージダイジェストと情報端末３０のアクセスログとがペアでデータ保存機能２３により保存される（ステップＳ２７）。

【００４９】

上述のごとく、公開立証システム１Ｂは、第１実施形態の公開立証システム１Ａと同様、閲覧者側の情報端末３０から情報提供サーバ１０上の公開情報をアクセスする場合、公開情報アクセスログ記録サーバ２０Ｂを経由してアクセスする仕組みとなっている。そして、公開情報アクセスログ記録サーバ２０Ｂでは、情報端末３０からアクセス・閲覧された公開情報の内容データから作成したメッセージダイジェストと、アクセス日時等を含むアクセスログとが、閲覧アクセスログとして保存される。

【００５０】

この場合、情報提供サーバ１０により公開・掲示された公開情報についてはその公開・掲示を終了した後も、公開情報保存機能１２により保存しておく必要がある。なぜならば、公開情報のメッセージダイジェストを公開の証拠として用いる際には、公開情報保存機能１２により保存しておいた公開情報から、メッセージダイジェスト生成機能２４で使用されたものと同じアルゴリズムによりメッセージダイジェストを生成し、生成されたメッセージダイジェストと閲覧アクセスログに含まれているメッセージダイジェストとをつき合わせ、全く同じメッセージダイジェストが生成されるか否かを確認する必要があるからである。

【００５１】

また、情報端末３０のアクセスログを、公開情報アクセスログ記録サーバ２０Ｂ側ではなく情報提供サーバ１０側で保存し、公開情報アクセスログ記録サーバ２０Ｂ側では、閲覧アクセスログのうちのメッセージダイジェストだけを保存してもよい。

例えば公開情報アクセスログ記録サーバ２０Ｂが複数の情報提供サーバ１０における公開情報の閲覧記録を管理するような場合、記憶媒体の容量を考えると、公開情報をそのまま保存するよりも、公開情報の内容データをメッセージダイジェストの形で保存しておく方が現実的である。

【００５２】

また、データ量の少ない、情報端末３０のアクセスログについてはそのままの状態で公開情報アクセスログ記録サーバ２０Ｂに保存することで、情報端末３０のアクセスログについて、情報提供サーバ１０における記録フォーマットと公開情報アクセスログ記録サーバ２０Ｂにおける記録フォーマットとを一致させる必要がなくなる。

【００５３】

従って、閲覧アクセスログのうち、公開情報データの内容のみをメッセージダイジェスト化して保存し、情報端末３０のアクセスログはそのまま保存するという組み合わせが実際的である。

以上のようにして、閲覧された公開情報データのメッセージダイジェストとアクセスログとをペアにし、閲覧アクセスログ（閲覧アクセス記録証拠データ群）として保存することにより、前記公開情報データが公開情報としてクセスが可能であったという証拠を残すことが可能になる。

【００５４】

このように、本発明の第２実施形態としての公開立証システム１Ｂや公開情報アクセスログ記録サーバ２０Ｂによれば、第１実施形態と同様の作用効果が得られるほか、公開情報データをメッセージダイジェストの形で保存することで、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

【００５５】

〔３〕第３実施形態の説明

図６は本発明の第３実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００５６】

図６に示すように、第３実施形態の公開立証システム１Ｃも、第２実施形態の公開立証システム１Ｂとほぼ同様に構成されているが、第３実施形態の公開立証システム１Ｃでは、第２実施形態の公開情報アクセスログ記録サーバ２０Ｂに代えて公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ）２０Ｃがそなえられている。この公開情報アクセスログ記録サーバ２０Ｃは、第２実施形態と同様のデータ送受信機能２１，データトラップ機能２２，データ保存機能２３およびメッセージダイジェスト生成機能２４のほかに、暗号化機能２５をさらに有している。

【００５７】

暗号化機能２５は、公開情報アクセスログ記録サーバ２０Ｃのデータ保存機能２３によって保存されるべき閲覧アクセスログを、公開情報アクセスログ記録サーバ２０Ｃの秘密鍵を用いて暗号化することにより、その閲覧アクセスログにデジタル署名を施すためのものである。

【００５８】

つまり、暗号化機能２５は、公開情報アクセスログ記録サーバ２０Ｃのデータ保存機能２３により閲覧アクセスログとして保存される、閲覧された公開情報データもしくはそのメッセージダイジェストと、その公開情報に対する閲覧アクセスを行なった情報端末３０のアクセスログもしくはそのメッセージダイジェストとに対して、公開情報アクセスログ記録サーバ２０Ｃの秘密鍵を使用してデジタル署名を行なうものである。ただし、第３実施形態における暗号化機能２５は、公開情報データのメッセージダイジェストと情報端末３０のアクセスログとを含む閲覧アクセスログに対して、公開情報アクセスログ記録サーバ２０Ｃの秘密鍵を使用してデジタル署名を行なうものとする。

【００５９】

なお、公開情報アクセスログ記録サーバ２０Ｃも、第１実施形態の公開情報アクセスログ記録サーバ２０Ａと同様、例えばパーソナルコンピュータ等の計算機により構成されており、データ送受信機能２１，データトラップ機能２２，データ保存機能２３，メッセージダイジェスト生成機能２４および暗号化機能２５は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【００６０】

次に、上述のごとく構成された第３実施形態の公開立証システム１Ｃおよび公開情報アクセスログ記録サーバ２０Ｃの動作について、図７に示すフローチャート（ステップＳ３１～Ｓ３８）に従って説明する。

情報提供サーバ１０における公開情報の閲覧を希望する者（閲覧者，第三者）は、第２実施形態と同様、情報端末３０（ＷＷＷブラウザ３２）を起動して通信ネットワーク２に接続し、情報提供サーバ１０に対する閲覧アクセスを、通信ネットワーク２を介して行なう（ステップＳ３１）。

【００６１】

そして、情報端末３０は、まず、公開情報アクセスログ記録サーバ２０Ｃにアクセスしてから（ステップＳ３２）、情報提供サーバ１０にアクセスし（ステップＳ３３）、情報提供サーバ１０における公開情報を閲覧することが可能な状態となる。

情報提供サーバ１０では、公開情報掲示機能１３により、情報端末３０からの指示に応じて、閲覧者の望む公開情報が、公開情報保存機能１２から検索されて読み出され、公開情報アクセスログ記録サーバ２０Ｃを経由して情報端末３０に返送され、閲覧者に提供される（ステップＳ３４）。

【００６２】

公開情報が公開情報アクセスログ記録サーバ２０Ｃを経由する際、公開情報アクセスログ記録サーバ２０Ｃにおいては、データトラップ機能２２により、閲覧者（第三者）が閲覧した公開情報と、その公開情報に対するアクセス日時を含む情報端末３０のアクセスログとが、閲覧アクセスログとしてトラップされ（ステップＳ３５）、トラップされた公開情報データのメッセージダイジェストが、メ

ッセージダイジェスト生成機能２４により作成される（ステップＳ３６）。

【００６３】

そして、第３実施形態においては、暗号化機能２５により、公開情報データのメッセージダイジェストと情報端末３０のアクセスログとからなる閲覧アクセスログが、公開情報アクセスログ記録サーバ２０Ｃの秘密鍵により暗号化されてデジタル署名を施されてから（ステップＳ３７）、デジタル署名を施された閲覧アクセスログがデータ保存機能２３により保存される（ステップＳ３８）。

【００６４】

上述のごとく、公開立証システム１Ｃは、第２実施形態の公開立証システム１Ｂと同様、閲覧者側の情報端末３０から情報提供サーバ１０上の公開情報をアクセスする場合、公開情報アクセスログ記録サーバ２０Ｃを経由してアクセスする仕組みとなっている。そして、公開情報アクセスログ記録サーバ２０Ｃでは、デジタル署名を施された閲覧アクセスログが保存される。

【００６５】

このように、本発明の第３実施形態としての公開立証システム１Ｃや公開情報アクセスログ記録サーバ２０Ｃによれば、第１および第２実施形態と同様の作用効果が得られるほか、閲覧アクセスログがデジタル署名を施されて保存されるので、閲覧アクセスログが改ざんされるのを確実に防止することができ、閲覧アクセスログの証拠能力をより高めることができる。

【００６６】

〔４〕第４実施形態の説明

図８は本発明の第４実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００６７】

図８に示すように、第４実施形態の公開立証システム１Ｄも、第３実施形態の公開立証システム１Ｃとほぼ同様に構成されているが、第４実施形態の公開立証システム１Ｄにおいては、第３実施形態と同様の情報提供サーバ１０および公開情報アクセスログ記録サーバ２０Ｃのほかに、第三者デジタル署名サーバ４０が

さらにそなえられている。

【００６８】

この第三者デジタル署名サーバ４０は、例えば電子公証会社に属するものであって、通信ネットワーク２を介して公開情報アクセスログ記録サーバ２０Ｃと通信可能に接続され、公開情報アクセスログ記録サーバ２０Ｃにおいてデジタル署名を施された閲覧アクセスログ（閲覧アクセス記録証拠データ群）に対しさらなるデジタル署名を施すべく、後述するデータ送受信機能４１，タイムスタンプ付加機能４２および暗号化機能４３を有している。

【００６９】

ここで、データ送受信機能４１は、通信ネットワーク２を介して、公開情報アクセスログ記録サーバ２０Ｃへ情報（例えばデジタル署名を施した閲覧アクセスログ等）を送信したり公開情報アクセスログ記録サーバ２０Ｃから情報（例えばデジタル署名を施すべき閲覧アクセスログ等）を受信したりするためのものである。

【００７０】

また、タイムスタンプ付加機能４２は、データ送受信機能４１により受信した情報（ここでは公開情報アクセスログ記録サーバ２０Ｃにおいてデジタル署名を施された閲覧アクセスログ）を受信すると、その閲覧アクセスログにタイムスタンプ（例えば、その閲覧アクセスログを受信した年月日および時刻）を付加するものである。

【００７１】

さらに、暗号化機能４３は、タイムスタンプを付加された閲覧アクセスログを、第三者デジタル署名サーバ４０の秘密鍵を用いて暗号化することにより、そのタイムスタンプ付き閲覧アクセスログにデジタル署名を施すものである。

そして、このようにデジタル署名を施されたタイムスタンプ付き閲覧アクセスログが、データ送受信機能４１により通信ネットワーク２を介して公開情報アクセスログ記録サーバ２０Ｃに返送され、データ保存機能２３によって保存されるようになっている。

【００７２】

なお、第三者デジタル署名サーバ４０に、暗号化機能４３によってデジタル署名を施された、タイムスタンプ付き閲覧アクセスログを保存するデータ保存機能（閲覧アクセスログ保存機能）４４をさらにそなえてもよい。この場合、デジタル署名を施された、タイムスタンプ付き閲覧アクセスログを、上述のごとく公開情報アクセスログ記録サーバ２０Ｃに返送してデータ保存機能２３にも保存させてもよいし、第三者デジタル署名サーバ４０のデータ保存機能４４にのみ保存してもよい。

【００７３】

次に、上述のごとく構成された第４実施形態の公開立証システム１Ｄおよび第三者デジタル署名サーバ４０の動作について、図９に示すフローチャート（ステップＳ３１～Ｓ３７およびＳ４１～Ｓ４６）に従って説明する。なお、図９に示すステップＳ３１～Ｓ３７の処理は図７に示したものと同様であるので、その説明は省略する。

【００７４】

第４実施形態においては、公開情報アクセスログ記録サーバ２０Ｃの暗号化機能２５によりデジタル署名を施された閲覧アクセスログ（閲覧アクセス記録証拠データ群）は、データ送受信機能２１により通信ネットワーク２を介して第三者デジタル署名サーバ４０に送信される（ステップＳ４１）。

【００７５】

そして、第三者デジタル署名サーバ４０のデータ送受信機能４１により、公開情報アクセスログ記録サーバ２０Ｃからの閲覧アクセスログが受信されると（ステップＳ４２）、受信したデータに対し、タイムスタンプ付加機能４２によりタイムスタンプが付加された後、タイムスタンプ付きの閲覧アクセスログが、暗号化機能４３により、第三者デジタル署名サーバ４０の秘密鍵により暗号化されてデジタル署名を施される（ステップＳ４３）。

【００７６】

この後、ステップＳ４３でデジタル署名（暗号化）を施された閲覧アクセスログは、データ送受信機能４１により通信ネットワーク２を介して公開情報アクセスログ記録サーバ２０Ｃに送信される（ステップＳ４４）。

そして、公開情報アクセスログ記録サーバ２０Ｃのデータ送受信機能２１により、第三者デジタル署名サーバ４０からの、暗号化済み閲覧アクセスログが受信されると（ステップＳ４５）、その暗号化済み閲覧アクセスログがデータ保存機能２３により保存される（ステップＳ４６）。

【００７７】

このように、本発明の第４実施形態としての公開立証システム１Ｄや第三者デジタル署名サーバ４０によれば、第１～第３実施形態と同様の作用効果が得られるほか、公開情報アクセスログ記録サーバ２０Ｃで得られた閲覧アクセスログにタイムスタンプを付加した状態で、第三者デジタル署名サーバ４０の秘密鍵を用いて、さらなるデジタル署名を施すことにより、この閲覧アクセスログが改ざんされるのをより確実に防止できるとともに、閲覧時刻にほぼ対応した日時（受信日時）がタイムスタンプとして付加されるので、閲覧アクセスログの証拠能力、つまりは証拠としての信頼性をより高めることができる。

【００７８】

なお、上述した第４実施形態では、閲覧アクセスログ（閲覧アクセス記録証拠データ群）に対して、公開情報アクセスログ記録サーバ２０Ｃと第三者デジタル署名サーバ４０との両方においてデジタル署名を施す場合について説明したが、公開情報アクセスログ記録サーバ２０Ｃでのデジタル署名を省略し、第三者デジタル署名サーバ４０でのデジタル署名のみを実行するように構成してもよい。

【００７９】

〔５〕第５実施形態の説明

図１０は本発明の第５実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

【００８０】

図１０に示すように、第５実施形態の公開立証システム１Ｅも、第４実施形態の公開立証システム１Ｄとほぼ同様に構成されているが、第５実施形態の公開立証システム１Ｅにおいては、第４実施形態と同様の情報提供サーバ１０，公開情報アクセスログ記録サーバ２０Ｃや第三者デジタル署名サーバ４０のほかに、複

数（図１０中では３個）の閲覧アクセス用情報端末５０がさらにそなえられている。

【００８１】

各閲覧アクセス用情報端末５０は、公開情報アクセスログ記録サーバ２０Ｃにおいて公開情報に対する閲覧アクセスログ（閲覧アクセス記録証拠データ群）を意図的に残すことを目的として、情報提供サーバ１０における公開情報に対する閲覧アクセスを定期的（所定の時間毎）に行なうもので、例えばパーソナルコンピュータ等の情報端末機器であり、後述するデータ送受信機能５１，ＷＷＷブラウザ５２，アクセス期日指定機能５３およびアクセスサイト指定データベース５４を有している。また、これらの情報端末５０は、例えば異なる複数の国にそれぞれ配置されているものとする。

【００８２】

ここで、データ送受信機能５１は、通信ネットワーク２を介し、公開情報アクセスログ記録サーバ２０Ａへ情報を送信したり公開情報アクセスログ記録サーバ２０Ａから情報を受信したりするためのものである。

ＷＷＷブラウザ（インターネットブラウザソフトウェア）５２は、通信ネットワーク２を介して即ちＷＷＷにより、情報提供サーバ１０に対する閲覧アクセス等を行なう際に用いられるものである。

【００８３】

アクセス期日指定機能５３は、情報端末５０が情報提供サーバ１０における公開情報に対してアクセス期日（期間，時間間隔）を指定するためのものであり、アクセスサイト指定データベース５４は、情報端末５０が閲覧アクセスを行なうべく指定されたアクセスサイト（即ち情報提供サーバ１０）のアドレスを予め保持するものである。

【００８４】

そして、情報端末５０のＷＷＷブラウザ５２が、アクセス期日指定機能５３によって指定されたアクセス期日に応じた所定の期間内の間、所定の時間毎に、アクセスサイト指定データベース５４に予め登録された情報提供サーバ１０の公開情報に対して、自動的に閲覧アクセスを行なうように構成されている。

【００８５】

次に、上述のごとく構成された第５実施形態の公開立証システム１Ｅおよび閲覧アクセス用情報端末５０の動作について、図１１に示すフローチャート（ステップＳ５１～Ｓ５９）に従って説明する。

閲覧アクセス用情報端末５０が起動されて通信ネットワーク２に接続されると（ステップＳ５１）、情報端末５０（ＷＷＷブラウザ５２）は、アクセス期日指定機能５３によって指定されたアクセス期日を参照するとともに（ステップＳ５２）、データベース５４を参照して、予め指定された情報提供サーバ１０のアドレスを読み出し（ステップＳ５３）、アクセス期日に応じた所定の期間内の間、所定の時間毎に、指定された情報提供サーバ１０の公開情報に対する閲覧アクセスを自動的に行なう（ステップＳ５４～Ｓ５６）。

【００８６】

このとき、情報端末５０は、前述した情報端末３０の場合と同様、まず、公開情報アクセスログ記録サーバ２０Ｃを経由して（ステップＳ５４）、情報提供サーバ１０にアクセスし（ステップＳ５５）、情報提供サーバ１０における公開情報を閲覧することが可能な状態となる。

そして、情報提供サーバ１０では、情報端末５０からの指示に応じて、公開情報掲示機能１３により、公開情報が公開情報保存機能１２から検索されて読み出され、公開情報アクセスログ記録サーバ２０Ｃを経由して情報端末５０に返送される（ステップＳ５６）。

【００８７】

これに伴って、公開情報アクセスログ記録サーバ２０Ｃおよび第三者デジタル署名サーバ４０により、図９に示すステップＳ３５～Ｓ３７およびＳ４１～Ｓ４６の処理が実行され、公開情報アクセスログ記録サーバ２０Ｃに閲覧アクセスログ（閲覧アクセス記録証拠データ群）が保存される（ステップＳ５７）。

この後、閲覧アクセス用情報端末５０は、閲覧アクセスについてのアクセスログを保存すると（ステップＳ５８）、通信ネットワーク２から切断され停止され（ステップＳ５９）、一連の閲覧アクセス処理を終了する。

【００８８】

上述のごとく、公開立証システム１Ｅでは、情報提供サーバ１０や公開情報アクセスログ記録サーバ２０Ｃが、閲覧者側の情報端末３０（図１等参照）からの閲覧アクセスが発生するのを待つのではなく、公開立証システム１Ｅの運用者側が、インターネット経由で情報提供サーバ１０における公開情報に対し、所定期間に亘って定期的にアクセスする情報端末５０を予め設置し、この情報端末５０により、公開情報に対する閲覧アクセスを積極的に発生させている。

【００８９】

これにより、閲覧アクセスログ（閲覧アクセス記録証拠データ群）が公開情報アクセスログ記録サーバ２０Ｃに積極的に残されることになり、アクセス期日として予め指定した期間に亘り、情報提供サーバ１０における公開情報が閲覧可能であったという証拠を確実に残すことが可能になる。

また、情報端末５０を海外に設置することで、他国からのアクセスも可能であったことを証明することができる。さらには、パリ条約加盟国全てに情報端末５０を設置して情報アクセスが可能であったことを記録することで、情報提供サーバ１０で開示していた情報を特許公知例情報として主張することも可能になる。

【００９０】

このように、本発明の第５実施形態としての公開立証システム１Ｅや閲覧アクセス用情報端末５０によれば、第１～第４実施形態と同様の作用効果が得られるほか、閲覧アクセス用情報端末５０が公開情報に対する閲覧アクセスを定期的に行なうことにより、公開情報アクセスログ記録サーバ２０Ｃにおいて公開情報に対する閲覧アクセスログが定期的に且つ自動的に記録・保存される。

【００９１】

従って、第三者（例えば、前述した情報端末３０）から公開情報に対する閲覧アクセスがなくても、閲覧アクセス用情報端末５０による閲覧アクセス期間を予め決めておけば、少なくともその期間について、その公開情報が電子データとして通信ネットワーク２上において誰でもまた海外からもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク２上で掲示・公開されていたことを確実に立証することができる。

【００９２】

これにより、通信ネットワーク２上で掲示・公開された情報に、より確実に、印刷物や出版物と同様の証拠能力をもたせることができる。

また、電子文書が作成された日付のみならず、その電子文書が公開情報として通信ネットワーク２経由で外部からアクセス可能であった時期と期間とを証明することが可能になる。

【００９３】

〔５－１〕第５実施形態の第１変形例の説明

図１２は本発明の第５実施形態としての公開立証システムの第１変形例の構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

図１２に示すように、第１変形例の公開立証システム１Ｅ－１も、第５実施形態の公開立証システム１Ｅとほぼ同様に構成されているが、第１変形例の公開立証システム１Ｅ－１においては、通信ネットワーク２と複数の閲覧アクセス用情報端末５０との間に、それぞれ、インターネットサービスプロバイダのサーバ３が介在している。つまり、各閲覧アクセス用情報端末５０が、インターネットサービスプロバイダのサーバ３を経由して通信ネットワーク２に接続されている。

【００９４】

次に、上述のごとく構成された第５実施形態の第１変形例の公開立証システム１Ｅ－１の動作について、図１３に示すフローチャート（ステップＳ５１～Ｓ６０）に従って説明する。なお、図１３に示すステップＳ５１～Ｓ５９の処理は図１１に示したものとほぼ同様であるので、その詳細な説明は省略する。

【００９５】

第５実施形態の第１変形例においては、各閲覧アクセス用情報端末５０が、公開情報アクセスログ記録サーバ２０Ｃを経由して情報提供サーバ１０の公開情報にアクセスする際に、インターネットサービスプロバイダのサーバ３を経由して通信ネットワーク２に接続されるため、前述したステップＳ５３とステップＳ５４との間で、新たなステップＳ６０の処理が実行されている。

【００９６】

つまり、図１３に示すように、ステップＳ５３の処理後、情報端末５０は、イ

ンターネットサービスプロバイダのサーバ３にダイヤルアップ接続され（ステップＳ６０）、そのサーバ３を通し、さらに通信ネットワーク２および公開情報アクセスログ記録サーバ２０Ｃを経由して情報提供サーバ１０にアクセスする（ステップＳ５４，Ｓ５５）。

【００９７】

なお、図１１に示したステップＳ５１では、情報端末５０が起動されて通信ネットワーク２に接続されているが、この第１変形例では、上述のごとく、ステップＳ５９において情報端末５０が通信ネットワーク２に接続されるようになっているため、図１３に示すステップＳ５１では、情報端末５０が起動されるだけである。

【００９８】

このようにして、所定のＷｅｂサイト（情報提供サーバ１０）に対して複数かつ多国籍のプロバイダから所定の公開情報アクセスログ記録サーバ２０Ｃを経由して各企業のＷｅｂサイトにアクセスする仕組みを構築することができる。

そして、公開情報アクセスログ記録サーバ２０Ｃに保存される閲覧アクセスログ（情報端末５０のアクセスログ）内に、プロバイダのサーバ３経由で閲覧アクセスが行なわれた旨の記録が残ることになるため、より信頼性の高いアクセス情報を残すことができる。つまり、特定のＩＰ（Internet Protocol）アドレスや通信ネットワークドメインからのアクセスではなく、メジャーなプロバイダのサーバ３を経由するダイヤルアップ接続で公開情報にアクセスする可能であったことを証明することができる。

【００９９】

〔５－２〕第５実施形態の第２変形例の説明

図１４は本発明の第５実施形態としての公開立証システムの第２変形例の構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

図１４に示すように、第２変形例の公開立証システム１Ｅ－２も、第５実施形態の公開立証システム１Ｅとほぼ同様に構成されているが、第２変形例の公開立証システム１Ｅ－２においては、インターネットサービスプロバイダのプロキシ

サーバ４が公開情報アクセスログ記録サーバ２０Ｃとしての機能を有している。

【０１００】

このような公開立証システム１Ｅ－２によれば、インターネットサービスプロバイダのプロキシサーバ４に、閲覧アクセスログ記録サーバ２０Ｃとしての機能を組み込むことにより、情報端末５０において一般に用いられるＷＷＷブラウザ（インタネットブラウザソフトウェア）５２により指定されるプロキシサーバを、閲覧アクセスログ記録サーバ２０Ｃとしての機能を有するプロキシサーバ４に変更するだけで、情報端末５０は公開立証システム１Ｅ－２を容易に利用することができるほか、インターネットサービスプロバイダが新しいサービスを容易に提供することも可能になる。

【０１０１】

さらには、各国に専用の情報端末５０を設置し、その情報端末５０から、所定の日時や時刻に、上述したプロキシサーバ４を経由してＷｅｂサイト（情報提供サーバ１０）に自動的にアクセスすることにより、プロキシサーバ４や第三者デジタル署名サーバ４０において、情報提供サーバ１０の公開情報が各国から閲覧可能であったという証拠を自動的に且つ確実に残すことが可能になる。

【０１０２】

〔６〕第６実施形態の説明

第６実施形態では、後で詳述するごとく、例えば、情報提供サーバ１０として発明技術公開サーバ６０（図１５参照）を設定する。

この発明技術公開サーバ６０では、サーバ運用者と利用契約を結んでいる契約者の発明技術情報を常に情報公開するようにする。契約者は特許権利化がグレーの領域にある発明を行なった場合に特許出願を行なう代わりに、匿名にて発明技術公開サーバ６０に公開情報として発明技術情報を掲載する。

【０１０３】

この情報を掲載する際には、運用者側は例えば契約者ＩＤとパスワードとでアクセス管理を行なう。このとき、運用者側は、例えば１件当たりの情報掲載料を課金・徴収する。

契約者側は、発明技術公開サーバ６０に技術を公開することで、自身の発明の

特許化は断念することになるが、他社が同様な特許を出願して権利化することを抑止することができる。また、従来の技術公開情報のように紙ベースではなく、電子ベースでの開示になるため、発案して即開示することも可能で、従来のように開示準備中に他者に特許出願されてしまう可能性も低く抑えることができる。

【０１０４】

つまり、近年のように細分化された特許が出願される状況では、会社によってはその出願費用が嵩む場合が出てくる。その反面、特許出願をしなくて、且つ、アイディアのままで保持している場合には、他社が出願した場合にその技術を使用することができなくなってしまう。

そこで、公開期間が証明され、且つ、誰でもアクセス可能な形で発明技術公開サーバ６０を運用することで、発明者にとっての最悪状況を回避させることができる。なお、匿名で情報を開示するのは、誰がどのような発明を行なっているかという技術開発動向を調査されることを回避するためである。

【０１０５】

さらには、契約者が発明技術公開サーバ６０に発明技術情報を掲載したときのアクセスログとデータ内容とを、第１～第５実施形態で説明したものと同様の手法で掲載アクセスログとして保存することにより、その発明技術情報がいつから掲載されているかの証拠も残すことが可能になる。また、その発明情報を何処の誰が掲載したかという情報についても、契約者ＩＤにより特定することが可能になる。

【０１０６】

図１５は本発明の第６実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

第６実施形態では、情報が公開情報であったことを立証する本発明の仕組み（公開立証システム）を、より具体的な例、即ち、上述したような、発明技術情報を一般に公開するためのシステムに適用した場合について説明する。

【０１０７】

従って、第６実施形態の公開立証システム１Ｆは、図１５に示すように、第５

実施形態の公開立証システム１Ｅとほぼ同様に構成されているが、第６実施形態の公開立証システム１Ｆにおいては、第５実施形態の情報提供サーバ１０に代えて発明技術公開サーバ６０がそなえられるとともに、第５実施形態の公開情報アクセスログ記録サーバ２０Ｃに代えて公開情報アクセスログ記録サーバ７０がそなえられている。

【０１０８】

なお、第６実施形態では、公開情報（ここでは発明技術情報）の掲載希望者がその情報を発明技術公開サーバ６０に送信・掲載するための掲載アクセス用情報端末８０がそなえられている。この掲載アクセス用情報端末８０は、例えばパーソナルコンピュータ等の情報端末機器であり、前述した情報端末３０や５０と同様のデータ送受信機能８１およびＷＷＷブラウザ（インターネットブラウザソフトウェア）８２を有するほか、前記発明技術情報を予め保存するための掲示用発明技術情報保存機能８３を有している。

【０１０９】

また、掲載希望者には、発明技術公開サーバ６０の運用者と予め利用契約を結ぶことにより、予め識別情報（利用者ＩＤ，契約者ＩＤ）とパスワード（パスフレーズ）とが付与されており、掲載希望者は、発明技術情報を情報端末８０から発明技術公開サーバ６０に送信して掲載する際には、それに先立ち、その識別情報およびパスワードを、情報端末８０から通信ネットワーク２を経由して発明技術公開サーバ６０に送信するようになっている。

【０１１０】

そして、発明技術公開サーバ（情報提供サーバ）６０は、データ送受信機能６１，発明技術情報保存機能６２，発明技術情報掲示機能６３，発明技術情報登録機能６４および課金情報更新機能６５を有している。

データ送受信機能６１，発明技術情報保存機能６２および発明技術情報掲示機能６３は、ぞれぞれ、前述したデータ送受信機能２１，公開情報保存機能２２および公開情報掲示機能２３に対応している。ただし、発明技術情報保存機能６２および発明技術情報掲示機能６３が、公開情報として、より具体的な発明技術情報を取り扱っている点だけが異なっている。

【０１１１】

また、発明技術情報登録機能６４は、情報端末８０から送信されてきた識別情報とパスワードとに基づいて掲載希望者の確認を行なった後、情報端末８０から送信されてきた発明技術情報を発明技術情報保存機能６２に登録して保存・掲載するためのものである。

さらに、課金情報更新機能６５は、発明技術情報登録機能６４により発明技術情報の登録を行なった場合、その情報の掲載者（契約者）から情報掲載料を徴収すべく、識別情報に対応した、掲載者についての課金情報更新するためのものである。

【０１１２】

なお、上述した発明技術公開サーバ６０も例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能６１，発明技術情報保存機能６２，発明技術情報掲示機能６３，発明技術情報登録機能６４および課金情報更新機能６５は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【０１１３】

一方、公開情報アクセスログ記録サーバ７０は、上述した機能２１～２５にそれぞれ対応する、データ送受信機能７１，データトラップ機能７２，データ保存機能７３，メッセージダイジェスト生成機能７４および暗号化機能７５を有している。

【０１１４】

ただし、第６実施形態における公開情報アクセスログ記録サーバ７０は、前述した公開情報アクセスログ記録サーバ２０Ｃと同様の機能つまり閲覧アクセスログ記録サーバとしての機能のほかに、情報端末８０からの発明技術情報の掲載アクセスに際し、発明技術情報のデータ内容とその掲載日時とを含む掲載アクセスログを獲得して保存する、掲載サクセスログ記録サーバとしての機能を併せもつものである。

【０１１５】

このため、データトラップ機能（閲覧アクセスログ獲得機能，掲載アクセスロ

グ保存機能）７２は、前述したデータトラップ機能２２と同様の機能を果たすほかに、情報端末８０から通信ネットワーク２を介して発明技術公開サーバ６０に送信・掲載される発明技術情報と、その掲載日時を含む、情報端末８０のアクセスログとを掲載アクセスログ（公開情報アクセスログ，掲載アクセス記録証拠データ群）として獲得する掲載アクセスログ獲得機能としての機能を果たすものである。

【０１１６】

つまり、データトラップ機能７２は、情報端末３０（図１５では図示省略）や情報端末５０から発明技術公開サーバ６０に対する閲覧アクセスが行なわれた場合、あるいは、情報端末８０から発明技術公開サーバ６０に対する掲載アクセスが行なわれた場合、これらの情報端末３０，５０，８０と発明技術公開サーバ６０との間で通信ネットワーク２を介してやり取りされるデータ群（公開情報アクセスログ記録サーバ７０を経由・通過するデータ群）から、上述した各種データを閲覧アクセスログあるいは掲載アクセスログとしてトラップするものである。

【０１１７】

なお、掲載アクセスログに含まれる、情報端末８０のアクセスログとしては、図２を参照しながら前述したもののほかに、発明技術情報を送信した情報端末８０にかかる端末情報、例えば、閲覧者（情報端末８０）側の通信ネットワークアドレス，氏名，アクセス経路や、前述した識別情報（契約者ＩＤ）などをさらに獲得してもよい。

【０１１８】

また、データ保存機能（閲覧アクセスログ保存機能，掲載アクセスログ保存機能）７３は、前述したデータ保存機能２３と同様、データトラップ機能７２によってトラップされた閲覧アクセスログもしくは掲載アクセスログを保存するためのものである。このデータ保存機能７３において、閲覧アクセスログもしくは掲載アクセスログは、データトラップ７２で獲得された形式のまま保存されてもよいが、本実施形態では、後述するメッセージダイジェスト生成機能７４，暗号化機能７５および第三者デジタル署名サーバ４０によって処理を施された形式で保存されるようになっている。

【０１１９】

メッセージダイジェスト生成機能７４は、例えばＭＤ５（Message Digest algorithm 5）等のアルゴリズムを使用して、データトラップ機能２２によりトラップされた発明技術情報のメッセージダイジェストを生成するものである。このとき、メッセージダイジェスト生成機能７４により、閲覧アクセスログや掲載アクセスログの全てについてのメッセージダイジェストを生成してもよい。

【０１２０】

このとき、データ保存機能７３においては、発明技術情報のメッセージダイジェストと、情報端末３０，５０，８０のアクセスログとをペアにして、閲覧アクセスログもしくは掲載アクセスログとして保存してもよいし、閲覧アクセスログや掲載アクセスログの全てについて生成されたメッセージダイジェストを保存してもよい。

【０１２１】

暗号化機能７５は、データ保存機能７３によって保存されるべき閲覧アクセスログもしくは掲載アクセスログを、公開情報アクセスログ記録サーバ７０の秘密鍵を用いて暗号化することにより、その閲覧アクセスログもしくは掲載アクセスログにデジタル署名を施すためのものである。

【０１２２】

このとき、データ保存機能７３においては、暗号化機能７５により、データトラップ機能７２で獲得された形式のままの、閲覧アクセスログもしくは掲載アクセスログを暗号化した結果を保存してもよいし、メッセージダイジェスト生成機能７４により生成されたメッセージダイジェストを含む閲覧アクセスログもしくは掲載アクセスログを暗号化した結果を保存してもよい。さらに、データ保存機能７３においては、第４実施形態で前述したように、第三者デジタル署名サーバ４０を用いて暗号化を施された閲覧アクセスログもしくは掲載アクセスログを保存してもよい。

【０１２３】

なお、上述した公開情報アクセスログ記録サーバ７０も例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能７１，デ

ータトラップ機能７２，データ保存機能７３，メッセージダイジェスト生成機能７４および暗号化機能７５は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

また、本実施形態では、公開情報アクセスログ記録サーバ７０が、閲覧アクセスログ記録サーバとしての機能と掲載アクセスログ記録サーバとしての機能とを併せもっているが、これらの機能をそれぞれ異なるサーバにそなえてもよい。

【０１２４】

次に、上述のごとく構成された第６実施形態の公開立証システム１Ｆ，発明技術公開サーバ６０および公開情報アクセスログ記録サーバ７０の動作について、図１６に示すフローチャート（ステップＳ６１～Ｓ７０）に従って説明する。

なお、発明技術公開サーバ６０によって掲示・公開される発明技術情報に対する閲覧アクセス、および、その閲覧アクセスに伴う閲覧アクセスログ（閲覧アクセス記録証拠データ群）の記録・保存は、前述した実施形態と同様にして行なわれるので、その説明は省略する。

【０１２５】

従って、ここでは、発明技術情報の掲載希望者（既に発明技術公開サーバ６０の運用者と利用契約を結んでいる契約者）が、その発明技術情報を発明技術公開サーバ６０に掲載する処理（掲載アクセス）について、図１６を参照しながら詳細に説明する。

【０１２６】

まず、掲載希望者は、掲載アクセス用情報端末８０を起動して（ステップＳ６１）、通信ネットワーク２に接続し（ステップＳ６２）、公開情報アクセスログ記録サーバ７０を経由して発明技術公開サーバ６０にアクセスし（ステップＳ６３）、この発明技術公開サーバ６０における発明技術掲載メニューにアクセスする（ステップＳ６４）。

【０１２７】

そして、掲載希望者は、発明技術掲載メニューの指示に従って、予め付与されている契約者ＩＤおよびパスワードを入力し（ステップＳ６５）、発明技術公開サーバ６０側において、入力された契約者ＩＤおよびパスワードに基づいて掲載

希望者が契約者である旨が確認されると、発明情報掲載メニューにログインする（ステップＳ６６）。

【０１２８】

ついで、掲載希望者は、発明技術公開サーバ６０での掲示・公開を希望する発明技術情報（発明データ）を、情報端末８０から公開情報アクセスログ記録サーバ７０を経由して発明技術公開サーバ６０に送信する（ステップＳ６７）。

このとき、公開情報アクセスログ記録サーバ７０および第三者デジタル署名サーバ４０により、例えば図９に示すステップＳ３５～Ｓ３７およびＳ４１～Ｓ４６と同様の処理が実行され、公開情報アクセスログ記録サーバ７０（もしくは第三者デジタル署名サーバ４０）に、発明技術情報の内容と、少なくとも掲載日時を含む情報端末８０のアクセスログとが、掲載アクセスログ（掲載アクセス記録証拠データ群）として保存される（ステップＳ６８）。

【０１２９】

この後、掲載アクセス用情報端末８０は、今回の掲載アクセスについてのアクセスログを保存すると（ステップＳ６９）、掲載希望者が、情報端末８０を通信ネットワーク２から切断して停止し（ステップＳ７０）、一連の掲載アクセス処理を終了する。

【０１３０】

このように、本発明の第６実施形態としての公開立証システム１Ｆ，発明技術公開サーバ６０および公開情報アクセスログ記録サーバ７０によれば、第１～第５実施形態と同様の作用効果が得られるほかに、以下のような作用効果が得られる。

（ａ）発明技術公開サーバ６０に送信・掲載された発明技術情報について、その内容と掲載日時とが掲載アクセスログとして公開情報アクセスログ記録サーバ７０もしくは第三者デジタル署名サーバ４０に記録・保存されるので、公開情報の掲載履歴を、掲載アクセスログにより証明可能な形式で保存することができるので、その掲載日時以降、その公開情報が電子データとして通信ネットワーク（インターネット）２上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク２上で掲示・公開されていたことを立証する

ことができる。従って、通信ネットワーク２上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる。

【０１３１】

（ｂ）上述のごとく電子データに印刷物や出版物と同様の証拠能力をもたせることが可能になったことで、通信ネットワーク（インターネット）２上で公開された電子データを例えば特許の公知例として採用することが可能になる。

このとき、技術開発側から考えた場合、確実に情報公開を行なえ且つその情報公開期間を立証できるサービスが上述のごとく提供されることで、他社が権利化することを恐れて瑣末なアイディア等を全て特許や実用新案として出願することがなくなり、企業の特許出願費用の削減と特許庁に対する負荷の軽減とを実現可能になる。

【０１３２】

（ｃ）匿名の形で新規技術の公開サービスを行なうことが可能になり、クライアントの企業は開発動向を知られることなく、新規技術を公知情報として公開することが可能になる。従って、各企業や個人は、特許になるかならないか分からない技術を公知情報として開示記録を残すことができ、そのような技術を無理やり特許として出願するのを抑止でき、特許出願にかかる費用を削減することが可能になる。

【０１３３】

（ｄ）従来の技術公開情報のように紙ベースではなく、電子ベースで発明技術情報が開示されるため、発案して即開示することも可能で、従来の印刷物の技術公開公報と比較してリリースまでの時間を大幅に短縮することができ、公開準備をしている間に他者に同様のアイディアを出願される危険性が減る。

（ｅ）上述のような公開立証システム１Ｆを用いることにより、発明技術公開サーバ６０側は、契約者ＩＤとパスワードとを用いて発明技術情報の掲載アクセス管理を行なうことができ、例えば公開情報１件ごとに情報掲載料を課金・徴収するといった、新たな情報掲載サービスを容易に提供することが可能になる。

【０１３４】

（ｆ）公開情報アクセスログ記録サーバ７０が、閲覧アクセスログ記録サーバ

が掲載アクセスログ記録サーバとしての機能を兼ねることにより、異なる２種類のサーバをそなえる必要がなくなり、公開立証システム１Ｆをより簡素に構成することができる。

【０１３５】

〔６－１〕第６実施形態の変形例の説明

第６実施形態の変形例は、発明技術情報を発明技術公開サーバ６０において掲示する際に情報掲載者についての匿名性をより高めたい場合に対応したものであり、契約者がプリペイドカードを購入し、そのプリペイドカードに記された識別情報（ＩＤ）とパスワードとを用いて発明技術公開サーバ６０の発明情報情報掲示機能６３にアクセスするための手法が示されている。このとき、発明技術公開サーバ６０では、同一ＩＤによるアクセス回数（情報掲載回数）をカウントし、そのカウント値が所定の回数に到達した時点で、発明技術情報掲載機能６３へのログインを止めるように構成してもよい。この場合は、契約者が発明技術情報を事前に第三者デジタル署名サーバもしくは電子公証サーバに送り、タイムスタンプを加えてデジタル署名を受けておくことが望ましい。

【０１３６】

図１７は本発明の第６実施形態としての公開立証システムの変形例の構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

図１７に示すように、第６実施形態の変形例の公開立証システム１Ｆ－１も、第６実施形態の公開立証システム１Ｆとほぼ同様に構成されているが、この公開立証システム１Ｆ－１では、第６実施形態の発明技術公開サーバ６０に代えて発明技術公開サーバ（情報提供サーバ）６０－１がそなえられている。この発明技術公開サーバ６０－１は、第６実施形態と同様のデータ送受信機能６１，発明技術情報保存機能６２，発明技術情報掲示機能６３および発明技術情報登録機能６４を有するとともに、課金情報更新機能６５に代えてプリペイド残高更新機能６６を有している。

【０１３７】

なお、公開立証システム１Ｆ－１では、発明技術公開サーバ６０の運用者によ

って、識別情報（ＩＤ）とパスワードとを記載したプリペイドカードが予め発行され、発明技術情報の掲載希望者は、そのプリペイドカードを予め購入することになる。

【０１３８】

そして、この変形例における発明技術情報登録機能６４は、情報端末８０から送信されてきた識別情報（ＩＤ）とパスワードとが、既に発行され且つ未だ全度数を使用していないプリペイドカードに記載されたものであることを確認することにより、掲載希望者の確認を行なった後、情報端末８０から送信されてきた発明技術情報を発明技術情報保存機能６２に登録して保存・掲載するようになっている。

【０１３９】

また、プリペイド残高更新機能６６は、プリペイドカードの残存度数（残り使用回数）を、発明技術情報の発明技術公開サーバ６０への掲載回数に対応・連動させるためのものである。なお、このプリペイド残高更新機能６６は、前述したごとく、同一ＩＤによるアクセス回数（情報掲載回数）をカウントするものとしてもよい。この場合、発明技術情報登録機能６４は、そのカウント値が所定の回数に到達した時点で、発明技術情報掲載機能６３へのログインを止めるように動作することになる。

【０１４０】

次に、上述のごとく構成された第６実施形態の変形例の公開立証システム１Ｆ－１の動作について、図１８に示すフローチャート（ステップＳ７１～Ｓ８３）に従って説明する。

公開立証システム１Ｆ－１では、前述した通り、発明技術公開サーバ６０の運用者が、識別情報（ＩＤ）とパスワードとを記載したプリペイドカードを発行しており、発明技術情報の掲載希望者は、そのプリペイドカードを購入して（ステップＳ７１）、ＩＤとパスワードとを取得する（ステップＳ７２）。

【０１４１】

そして、掲載希望者は、掲載アクセス用情報端末８０を起動して（ステップＳ７３）、通信ネットワーク２に接続し（ステップＳ７４）、公開情報アクセスロ

グ記録サーバ７０を経由して発明技術公開サーバ６０にアクセスし（ステップＳ７５）、この発明技術公開サーバ６０における発明技術掲載メニューにアクセスする（ステップＳ７６）。

【０１４２】

そして、掲載希望者は、発明技術掲載メニューの指示に従って、購入したプリペイドカードに記載されたＩＤおよびパスワードを入力し（ステップＳ７７）、発明技術公開サーバ６０側において、入力されたＩＤおよびパスワードが、既に発行され且つ未だ全度数を使用していないプリペイドカードに記載されたものであることが確認されると、発明情報掲載メニューにログインする（ステップＳ７８）。

【０１４３】

ついで、掲載希望者は、発明技術公開サーバ６０での掲示・公開を希望する発明技術情報（発明データ）を、情報端末８０から公開情報アクセスログ記録サーバ７０を経由して発明技術公開サーバ６０に送信される（ステップＳ７９）。これに応じて、発明技術公開サーバ６０において、その発明技術情報が、発明技術情報登録機能６４によって発明技術情報保存機能６２に登録されると、プリペイド残高更新機能６６により、当該ＩＤを付与されたプリペイドカードについて、残存度数（残り使用回数）を減じるように度数の更新が行なわれる（ステップＳ８０）。

【０１４４】

また、このとき、公開情報アクセスログ記録サーバ７０および第三者デジタル署名サーバ４０により、例えば図９に示すステップＳ３５～Ｓ３７およびＳ４１～Ｓ４６と同様の処理が実行され、公開情報アクセスログ記録サーバ７０（もしくは第三者デジタル署名サーバ４０）に、発明技術情報の内容と、少なくとも掲載日時を含む情報端末８０のアクセスログとが、掲載アクセスログ（掲載アクセス記録証拠データ群）として保存される（ステップＳ８１）。

【０１４５】

この後、掲載アクセス用情報端末８０は、今回の掲載アクセスについてのアクセスログを保存すると（ステップＳ８２）、掲載希望者が、情報端末８０を通信

ネットワーク２から切断して停止し（ステップＳ８３）、一連の掲載アクセス処理を終了する。

【０１４６】

このようにな公開立証システム１Ｆ－１によれば、発明技術情報の掲載料を徴収した後に、掲載希望者の、より高い匿名性を確保しながら発明技術情報を発明技術公開サーバ６０で公開することができる。従って、匿名での情報掲載サービスを提供することも可能になる。

【０１４７】

〔７〕その他

なお、本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。

例えば、上述した第６実施形態では、公開情報が発明技術情報である場合について説明したが、本発明は、これに限定されるものではない。

【０１４８】

〔８〕付記

（付記１）　提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとをそなえたことを特徴とする、公開立証システム。

【０１４９】

（付記２）　該閲覧アクセスログ獲得機能が、該閲覧アクセスログとして、さらに、該公開情報にアクセスした該情報端末にかかる端末情報を獲得することを特徴とする、付記１記載の公開立証システム。

（付記３）　該閲覧アクセスログ記録サーバが、さらに、該閲覧アクセスロ

グ獲得機能により獲得された該公開情報のメッセージダイジェストを生成するメッセージダイジェスト生成機能を有し、

該閲覧アクセスログ保存機能が、該メッセージダイジェストを該閲覧アクセスログにおける該公開情報として保存することを特徴とする、付記１または付記２に記載の公開立証システム。

【０１５０】

（付記４）　一つのサーバが、該情報提供サーバとしての機能と該閲覧アクセスログ記録サーバとしての機能との両方を果たすように構成されていることを特徴とする、付記１～付記３のいずれか一つに記載の公開立証システム。

（付記５）　該閲覧アクセスログ記録サーバが、さらに、該閲覧アクセスログ保存機能によって保存されるべき該閲覧アクセスログを、該閲覧アクセスログ記録サーバの秘密鍵を用いて暗号化することにより、該閲覧アクセスログにデジタル署名を施す暗号化機能を有していることを特徴とする、付記１～付記４のいずれか一つに記載の公開立証システム。

【０１５１】

（付記６）　該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、所定の秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能とを有するデジタル署名サーバをさらにそなえ、

該閲覧アクセスログ記録サーバの該閲覧アクセスログ保存機能が、該デジタル署名サーバにおいてデジタル署名を施された、該タイムスタンプ付き閲覧アクセスログを保存することを特徴とする、付記１～付記５のいずれか一つに記載の公開立証システム。

【０１５２】

（付記７）　該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、所定の秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能と、該暗号化機能によってデジタル署名を施された、該タイムスタンプ付き閲覧アクセスログを保存する閲覧アクセスログ保存機

能とを有するデジタル署名サーバをさらにそなえたことを特徴とする、付記１～付記５のいずれか一つに記載の公開立証システム。

【０１５３】

（付記８）　該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なう、少なくとも一つの閲覧アクセス用情報端末をさらにそなえたことを特徴とする、付記１～付記７のいずれか一つに記載の公開立証システム。

【０１５４】

（付記９）　複数の該閲覧アクセス用情報端末が、複数の国にそれぞれ配置されていることを特徴とする、付記８記載の公開立証システム。

（付記１０）　該閲覧アクセス用情報端末が、インターネットサービスプロバイダのサーバを経由して該通信ネットワークに接続されていることを特徴とする、付記８または付記９に記載の公開立証システム。

【０１５５】

（付記１１）　インターネットサービスプロバイダのプロキシサーバが、該閲覧アクセスログ記録サーバとしての機能を有していることを特徴とする、付記１～付記１０のいずれか一つに記載の公開立証システム。

（付記１２）　該公開情報の掲載希望者が、該掲載希望者に対し予め付与された識別情報とパスワードとを、該通信ネットワークを介して該情報提供サーバに送信し、該情報提供サーバが、該識別情報と該パスワードとに基づき該掲載希望者の確認を行なった後に、該公開情報を保存・掲載することを特徴とする、付記１～付記１１のいずれか一つに記載の公開立証システム。

【０１５６】

（付記１３）　該識別情報と該パスワードとが、該掲載希望者によって購入されたプリペイドカードに記載されたものであることを特徴とする、付記１２記載の公開立証システム。

（付記１４）　該プリペイドカードの残存度数を、公開情報の該情報提供サーバへの掲載回数に対応させたことを特徴とする、付記１３記載の公開立証シス

テム。

【０１５７】

（付記１５）　該公開情報が該通信ネットワークを介して該情報提供サーバに掲載される際に該公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有する掲載アクセスログ記録サーバをさらにそなえたことを特徴とする、付記１～付記１４のいずれか一つに記載の公開立証システム。

【０１５８】

（付記１６）　該閲覧アクセスログ記録サーバが該掲載アクセスログ記録サーバとしての機能を兼ね、該閲覧アクセスログ獲得機能が該掲載アクセスログ記録サーバとして機能するとともに、該閲覧アクセスログ保存機能が該掲載アクセスログ保存機能として機能するように構成されたことを特徴とする、付記１５記載の公開立証システム。

【０１５９】

（付記１７）　該閲覧アクセスログ記録サーバの閲覧アクセスログ保存機能が、該閲覧アクセスログに含まれる該公開情報を圧縮した形で保存していることを特徴とする、付記１～付記１６のいずれか一つに記載の公開立証システム。

（付記１８）　通信ネットワークを介して閲覧された公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有することを特徴とする、閲覧アクセスログ記録サーバ。

【０１６０】

（付記１９）　該閲覧アクセスログ獲得機能が、該閲覧アクセスログとして、さらに、該公開情報にアクセスした該情報端末にかかる端末情報を獲得することを特徴とする、付記１８記載の閲覧アクセスログ記録サーバ。

（付記２０）　該閲覧アクセスログ獲得機能により獲得された該公開情報のメッセージダイジェストを生成するメッセージダイジェスト生成機能をさらに有

し、

該閲覧アクセスログ保存機能が、該メッセージダイジェストを該閲覧アクセスログにおける該公開情報として保存することを特徴とする、付記１８または付記１９に記載の閲覧アクセスログ記録サーバ。

【０１６１】

（付記２１）　該閲覧アクセスログ保存機能によって保存されるべき該閲覧アクセスログを、該閲覧アクセスログ記録サーバの秘密鍵を用いて暗号化することにより、該閲覧アクセスログにデジタル署名を施す暗号化機能をさらに有していることを特徴とする、付記１８～付記２０のいずれか一つに記載の閲覧アクセスログ記録サーバ。

【０１６２】

（付記２２）　通信ネットワークを介して情報提供サーバに送信・掲載された公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有することを特徴とする、掲載アクセスログ記録サーバ。

【０１６３】

（付記２３）　提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成するデジタル署名サーバであって、

該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、該デジタル署名サーバの秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログ

にデジタル署名を施す暗号化機能とを有することを特徴とする、デジタル署名サーバ。

【０１６４】

（付記２４）　該暗号化機能によってデジタル署名を施された、該タイムスタンプ付き閲覧アクセスログを保存する閲覧アクセスログ保存機能をさらに有することを特徴とする、付記２３記載のデジタル署名サーバ。

（付記２５）　提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成する情報端末であって、

該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なうことを特徴とする、閲覧アクセス用情報端末。

【０１６５】

【発明の効果】

以上詳述したように、本発明の公開立証システム（請求項１）並びに閲覧アクセスログ記録サーバ（請求項２），掲載アクセスログ記録サーバ（請求項３）およびデジタル署名サーバ（請求項４）並びに閲覧アクセス用情報端末（請求項５）によれば、以下のような効果ないし利点を得ることができる。

【０１６６】

（１）第三者により閲覧された公開情報について、その内容と閲覧日時とが閲覧アクセスログとして記録されるので、公開情報の公開履歴を、閲覧アクセスログにより証明可能な形式で保存することができ、少なくともその閲覧日時には、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可

能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。従って、通信ネットワーク上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる（請求項１，２）。

【０１６７】

（２）情報提供サーバに送信・掲載された公開情報について、その内容と掲載日時とが掲載アクセスログとして記録されるので、公開情報の掲載履歴を、掲載アクセスログにより証明可能な形式で保存することができ、その掲載日時以降、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。従って、通信ネットワーク上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる（請求項３）。

【０１６８】

（３）第三者である電子公証会社等のデジタル署名サーバにおいて、閲覧アクセスログ記録サーバで得られた閲覧アクセスログにタイムスタンプを付加した状態で、デジタル署名サーバの秘密鍵を用いてデジタル署名を施すことにより、この閲覧アクセスログが改ざんされるのを確実に防止できるほか、閲覧時刻にほぼ対応した日時がタイムスタンプとして付加されるので、閲覧アクセスログの証拠能力、つまりは証拠としての信頼性をより高めることができる（請求項４）。

【０１６９】

（４）閲覧アクセス用情報端末が公開情報に対する閲覧アクセスを定期的に行なうことにより、閲覧アクセスログ記録サーバにおいて公開情報に対する閲覧アクセスログが定期的に且つ自動的に記録・保存される。従って、第三者から公開情報に対する閲覧アクセスがなかった場合であっても、閲覧アクセス用情報端末による閲覧アクセス期間を予め決めておけば、少なくともその期間については、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを確実に立証することができる。これにより、通信ネットワー

ク上で掲示・公開された情報に、より確実に、印刷物や出版物と同様の証拠能力をもたせることができる（請求項５）。

【０１７０】

（５）上述のごとく電子データに印刷物や出版物と同様の証拠能力をもたせることが可能になったことで、通信ネットワーク上で公開された電子データを例えば特許の公知例として採用することが可能になる。これにより、加熱し瑣末化する特許競争に伴って増加していた、企業の特許出願に係る費用を減らすことができるとともに、特許庁に無用の負担をかけることがなくなる。

【０１７１】

（６）上述のごとく電子データに印刷物や出版物と同様の証拠能力をもたせることが可能になったことで、ビジネス上、以下のような意義がある。

（６－１）電子公証だけでなく、情報開示の開示記録や、アクセスが可能であったことの証明を行なうサービスを提供することができ、新規ビジネス創出の可能性が大きく広がる。

【０１７２】

（６－２）匿名の形で新規技術の公開サービスを行なうことで、クライアントの企業は開発動向を知られることなく、新規技術を公知情報として公開することが可能になる。従って、特許になるかならないか分からない技術を無理やり特許として出願するのを抑止でき、特許出願にかかる費用を削減することが可能になる。

（６－３）従来の印刷物の技術公開公報と比較してリリースまでの時間（情報を公開するまでにかかる時間）を大幅に短縮することができるため、公開準備をしている間に他者に同様のアイディアを出願される危険性が減る。

【０１７３】

（７）電子データが通信ネットワーク上で第三者が閲覧可能な状態で公開されていた日時を立証するサービスを提供することで、様々な局面で電子データを証拠として使用することが可能になる。

（８）閲覧アクセスログとして、公開情報にアクセスした情報端末にかかる端末情報を獲得し保存することにより、閲覧アクセスログに含まれる端末情報に基

づいて、どの情報端末がどのような経路で公開情報に対して閲覧アクセスを行なったかを特定することが可能になり、閲覧アクセスログの証拠能力をより高めることができる。

【０１７４】

（９）公開情報のメッセージダイジェストを生成し、このメッセージダイジェストを閲覧アクセスログにおける公開情報として保存することにより、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

（１０）一つのサーバを、情報提供サーバおよび閲覧アクセスログ記録サーバとして兼用することにより、２種類のサーバを別々にそなえる必要がなくなり、公開立証システムを簡素に構成することができる。

【０１７５】

（１１）閲覧アクセスログ記録サーバにおいて、閲覧アクセスログにデジタル署名を施して保存することにより、この閲覧アクセスログが改ざんされるのを確実に防止することができ、閲覧アクセスログの証拠能力を高めることが可能になる。

（１２）複数の閲覧アクセス用情報端末を複数の国にそれぞれ配置することにより、情報提供サーバにおける公開情報が複数の国から閲覧アクセス可能であったことを確実に証拠（閲覧アクセスログ）として残すことが可能になる。

【０１７６】

（１３）閲覧アクセス用情報端末がインターネットサービスプロバイダのサーバを経由して閲覧アクセスを行なうように構成することにより、閲覧アクセスログだけでなく、そのプロバイダのサーバにおいてアクセス記録が自動的に残るため、より信頼性の高いアクセス情報を残すことができる。

【０１７７】

（１４）インターネットサービスプロバイダのプロキシサーバに、閲覧アクセスログ記録サーバとしての機能を組み込むことにより、情報端末において一般に用いられるインタネットブラウザソフトウェアにより指定されるプロキシサーバを、閲覧アクセスログ記録サーバとしての機能を有するプロキシサーバに変更す

るだけで、情報端末は本発明の公開立証システムを容易に利用することができるほか、インターネットサービスプロバイダが新しいサービスを容易に提供することも可能になる。

【０１７８】

（１５）公開情報の掲載希望者が、その掲載希望者に対し予め付与された識別情報とパスワードとを、通信ネットワークを介して情報提供サーバに送信し、情報提供サーバが、識別情報とパスワードとに基づき掲載希望者の確認を行なった後に、公開情報を掲載するように構成することで、情報提供サーバ側は、その識別情報とパスワードとを用いて公開情報の掲載アクセス管理を行なうことができ、例えば公開情報１件ごとに情報掲載料を徴収するといった、新たな情報掲載サービスを容易に提供することが可能になる。

【０１７９】

（１６）識別情報とパスワードとが掲載希望者によって購入されたプリペイドカードに記載されたものとし、また、プリペイドカードの残存度数を、公開情報の情報提供サーバへの掲載回数に対応させることで、公開情報の掲載料を徴収した後に、掲載希望者のより高い匿名性を確保しながら公開情報を情報提供サーバで公開することができる。従って、匿名での情報掲載サービスを提供することも可能になる。

【０１８０】

（１７）閲覧アクセスログ記録サーバが掲載アクセスログ記録サーバとしての機能を兼ね、閲覧アクセスログ獲得機能が掲載アクセスログ記録サーバとして機能するとともに、閲覧アクセスログ保存機能が掲載アクセスログ保存機能として機能するように構成することにより、２種類のサーバを別々にそなえる必要がなくなり、公開立証システムを簡素に構成することができる。

【０１８１】

（１８）閲覧アクセスログ記録サーバの閲覧アクセスログ保存機能が、閲覧アクセスログに含まれる公開情報を圧縮した形で保存することにより、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態としての公開立証システムの構成を示すブロック図である。

【図２】

本実施形態において獲得・保存されるアクセスログの例を説明するための図である。

【図３】

第１実施形態の動作を説明するためのフローチャートである。

【図４】

本発明の第２実施形態としての公開立証システムの構成を示すブロック図である。

【図５】

第２実施形態の動作を説明するためのフローチャートである。

【図６】

本発明の第３実施形態としての公開立証システムの構成を示すブロック図である。

【図７】

第３実施形態の動作を説明するためのフローチャートである。

【図８】

本発明の第４実施形態としての公開立証システムの構成を示すブロック図である。

【図９】

第４実施形態の動作を説明するためのフローチャートである。

【図１０】

本発明の第５実施形態としての公開立証システムの構成を示すブロック図である。

【図１１】

第５実施形態の動作を説明するためのフローチャートである。

【図１２】

本発明の第５実施形態としての公開立証システムの第１変形例の構成を示すブロック図である。

【図１３】

第５実施形態の第１変形例の動作を説明するためのフローチャートである。

【図１４】

本発明の第５実施形態としての公開立証システムの第２変形例の構成を示すブロック図である。

【図１５】

本発明の第６実施形態としての公開立証システムの構成を示すブロック図である。

【図１６】

第６実施形態の動作を説明するためのフローチャートである。

【図１７】

本発明の第６実施形態としての公開立証システムの変形例の構成を示すブロック図である。

【図１８】

第６実施形態の変形例の動作を説明するためのフローチャートである。

【符号の説明】

１Ａ，１Ｂ，１Ｃ，１Ｄ，１Ｅ，１Ｅ－１，１Ｅ－２，１Ｆ，１Ｆ－１　公開立証システム

２　通信ネットワーク（インターネット）

３　インターネットサービスプロバイダのサーバ

４　インターネットサービスプロバイダのプロキシサーバ

１０　情報提供サーバ

１１　データ送受信機能

１２　公開情報保存機能

１３　公開情報掲示機能

２０Ａ，２０Ｂ，２０Ｃ　公開情報アクセスログ記録サーバ（閲覧アクセスロ

グ記録サーバ）

２１　データ送受信機能

２２　データトラップ機能（閲覧アクセスログ獲得機能）

２３　データ保存機能（閲覧アクセスログ保存機能）

２４　メッセージダイジェスト生成機能

２５　暗号化機能

３０　情報端末

３１　データ送受信機能

３２　WWWブラウザ（インターネットブラウザソフトウェア）

４０　第三者デジタル署名サーバ

４１　データ送受信機能

４２　タイムスタンプ付加機能

４３　暗号化機能

４４　データ保存機能（閲覧アクセスログ保存機能）

５０　閲覧アクセス用情報端末

５１　データ送受信機能

５２　WWWブラウザ（インターネットブラウザソフトウェア）

５３　アクセス期日指定機能

５４　アクセスサイト指定データベース

６０，６０－１　発明技術公開サーバ（情報提供サーバ）

６１　データ送受信機能

６２　発明技術情報保存機能（公開情報保存機能）

６３　発明技術情報掲示機能（公開情報掲示機能）

６４　発明技術情報登録機能

６５　課金情報更新機能

６６　プリペイド残高更新機能

７０　公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ，掲載サクセスログ記録サーバ）

７１　データ送受信機能

７２　データトラップ機能（閲覧アクセスログ獲得機能，掲載アクセスログ保存機能）

７３　データ保存機能（閲覧アクセスログ保存機能，掲載アクセスログ保存機能）

７４　メッセージダイジェスト生成機能

７５　暗号化機能

８０　掲載アクセス用情報端末

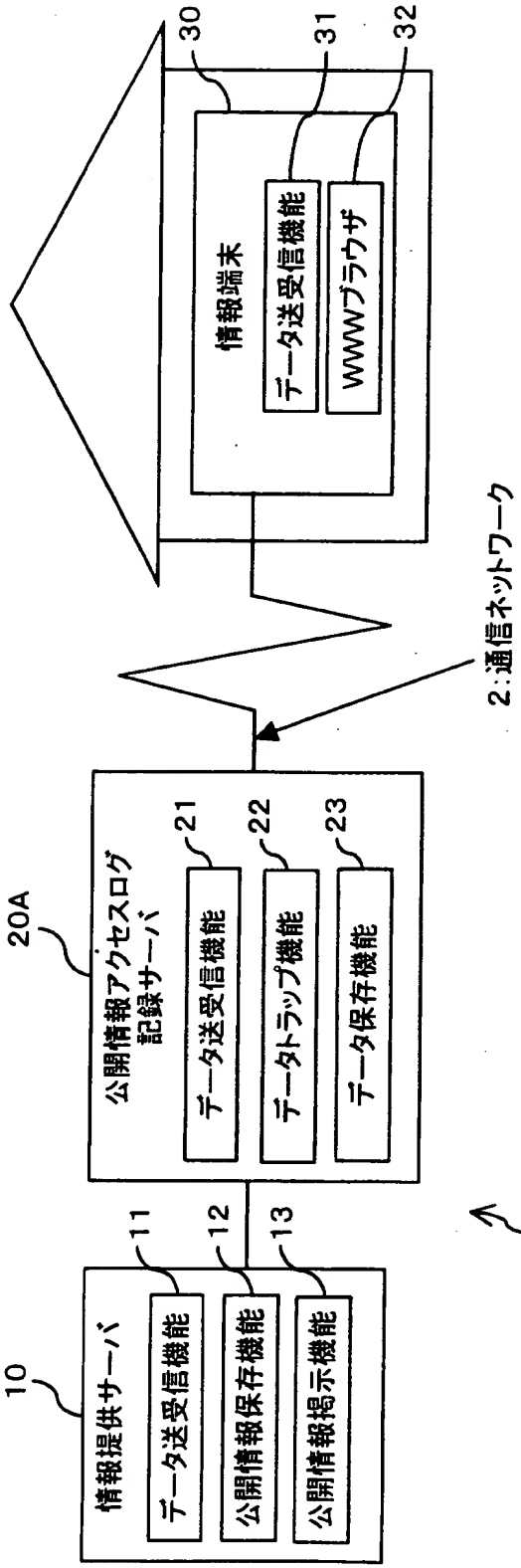
８１　データ送受信機能

８２　WWWブラウザ（インターネットブラウザソフトウェア）

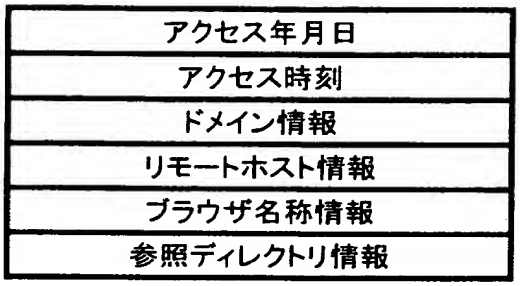
８３　掲示用発明技術情報保存機能

【書類名】　　図面

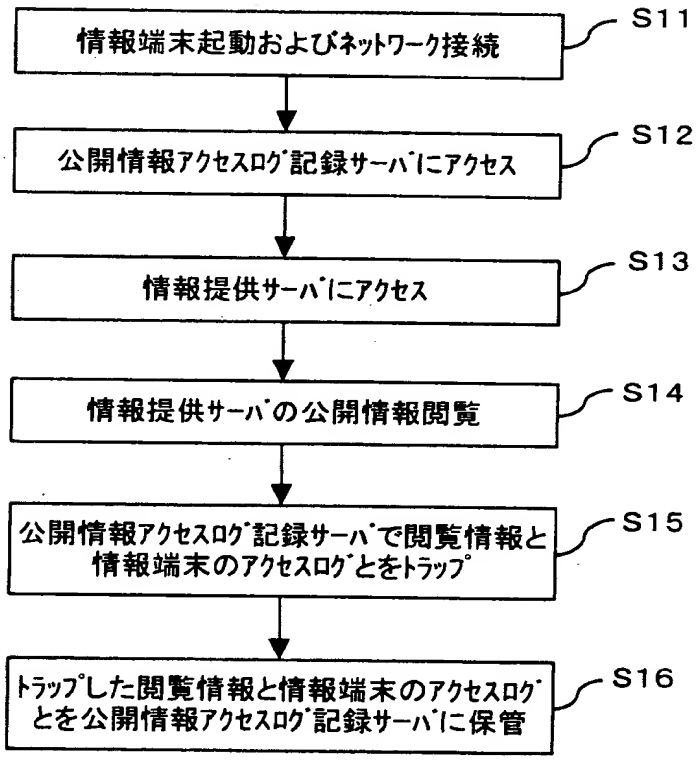
【図１】


30
31
32
情報端末
データ送受信機能
WWWブラウザ
2:通信ネットワーク
20A
公開情報アクセスログ
記録サーバ
21
22
23
データ送受信機能
データトラップ機能
データ保存機能
11
12
13
10
情報提供サーバ
データ送受信機能
公開情報保存機能
公開情報掲示機能
1A:公開立証システム

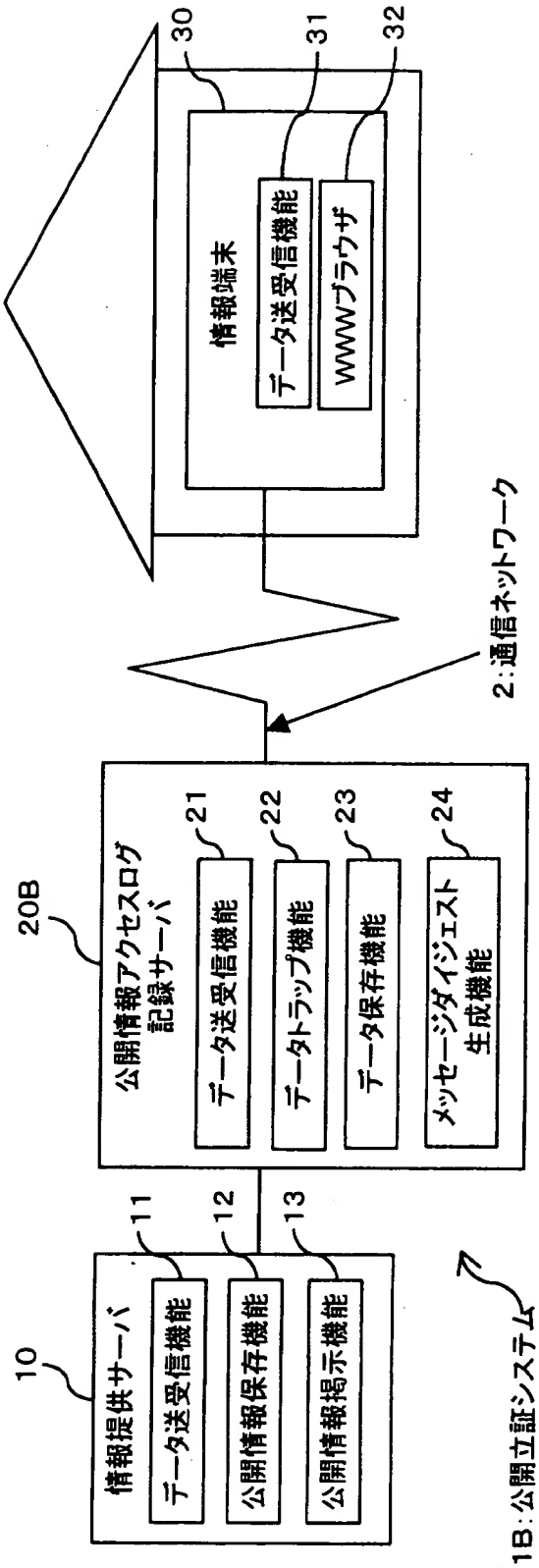
【図２】


アクセス年月日
アクセス時刻
ドメイン情報
リモートホスト情報
ブラウザ名称情報
参照ディレクトリ情報

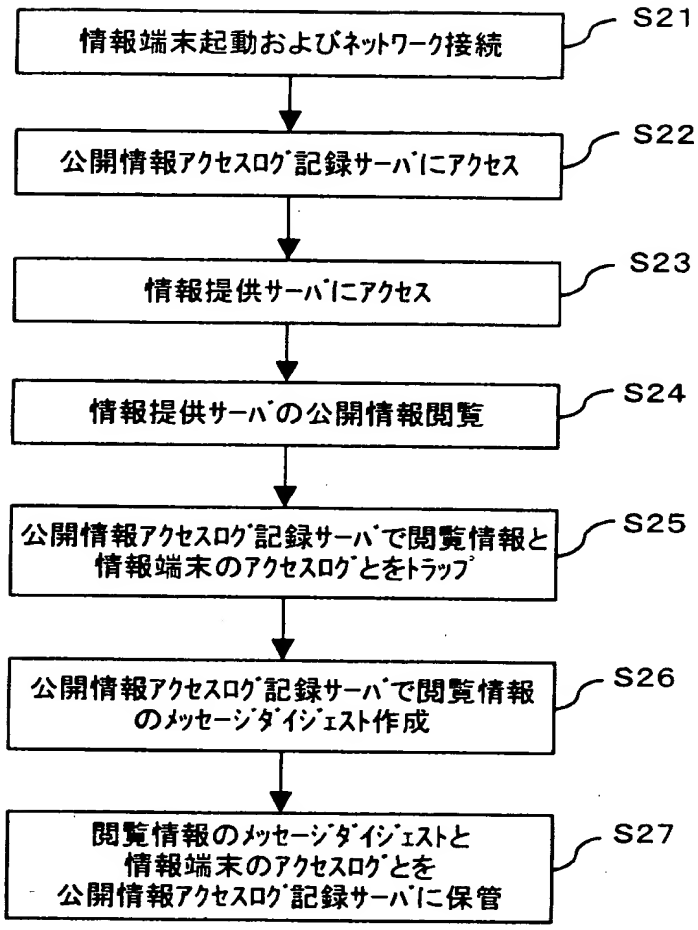
【図３】


情報端末起動およびネットワーク接続
S11
公開情報アクセスログ記録サーバにアクセス
S12
情報提供サーバにアクセス
S13
情報提供サーバの公開情報閲覧
S14
公開情報アクセスログ記録サーバで閲覧情報と情報端末のアクセスログとをトラップ
S15
トラップした閲覧情報と情報端末のアクセスログとを公開情報アクセスログ記録サーバに保管
S16

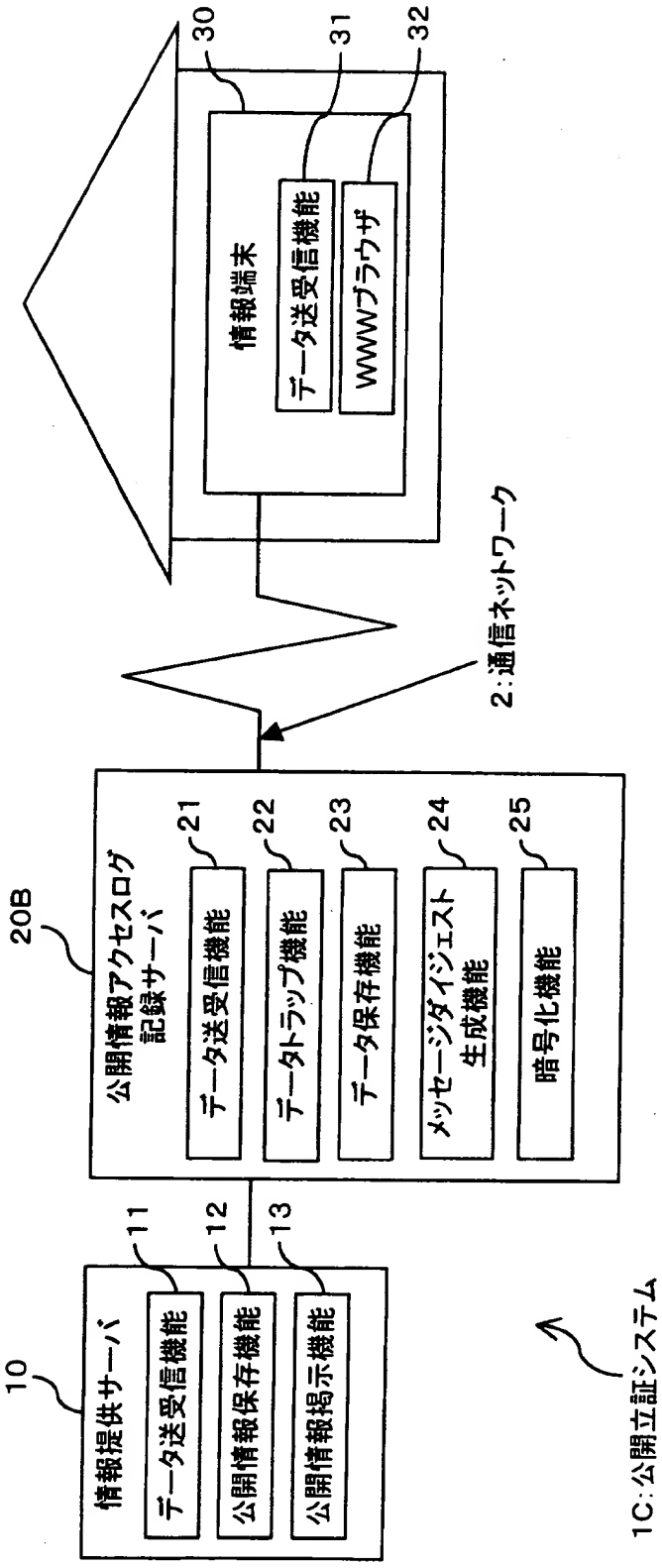
【図４】


30
31
32
情報端末
データ送受信機能
WWWブラウザ
2:通信ネットワーク
20B
公開情報アクセスログ
記録サーバ
21
22
23
24
データ送受信機能
データトラップ機能
データ保存機能
メッセージダイジェスト
生成機能
10
情報提供サーバ
11
12
13
データ送受信機能
公開情報保存機能
公開情報掲示機能
1B:公開立証システム

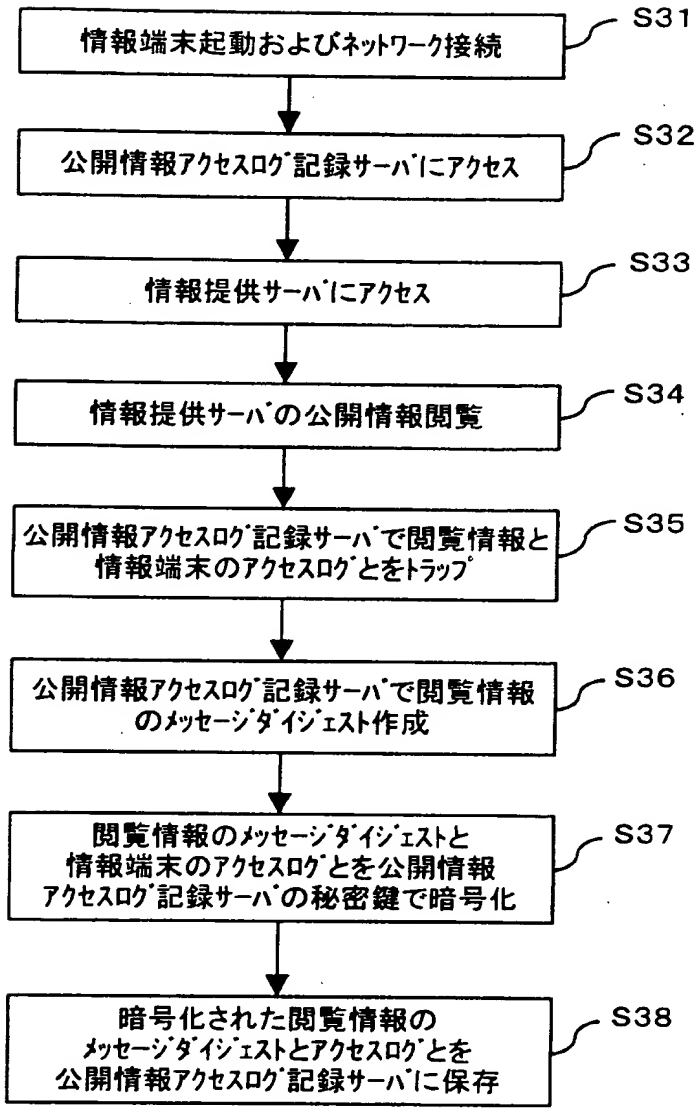
【図５】


情報端末起動およびネットワーク接続
S21
公開情報アクセスログ記録サーバにアクセス
S22
情報提供サーバにアクセス
S23
情報提供サーバの公開情報閲覧
S24
公開情報アクセスログ記録サーバで閲覧情報と情報端末のアクセスログとをトラップ
S25
公開情報アクセスログ記録サーバで閲覧情報のメッセージダイジェスト作成
S26
閲覧情報のメッセージダイジェストと情報端末のアクセスログとを公開情報アクセスログ記録サーバに保管
S27

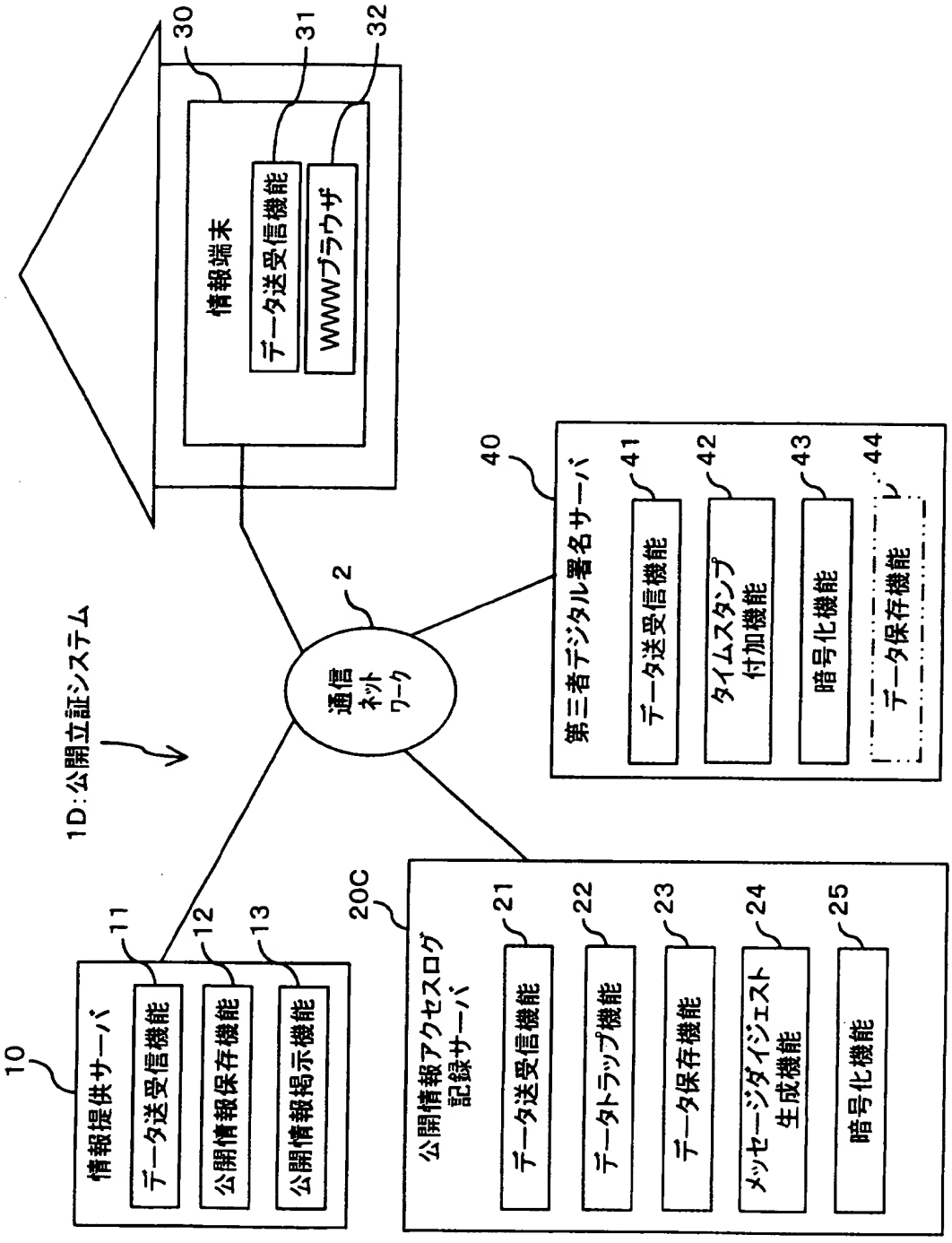
【図６】


30
31
32
情報端末
データ送受信機能
WWWブラウザ
2:通信ネットワーク
20B
公開情報アクセスログ
記録サーバ
21
22
23
24
25
データ送受信機能
データトラップ機能
データ保存機能
メッセージダイジェスト
生成機能
暗号化機能
10
情報提供サーバ
11
12
13
データ送受信機能
公開情報保存機能
公開情報掲示機能
1C:公開立証システム

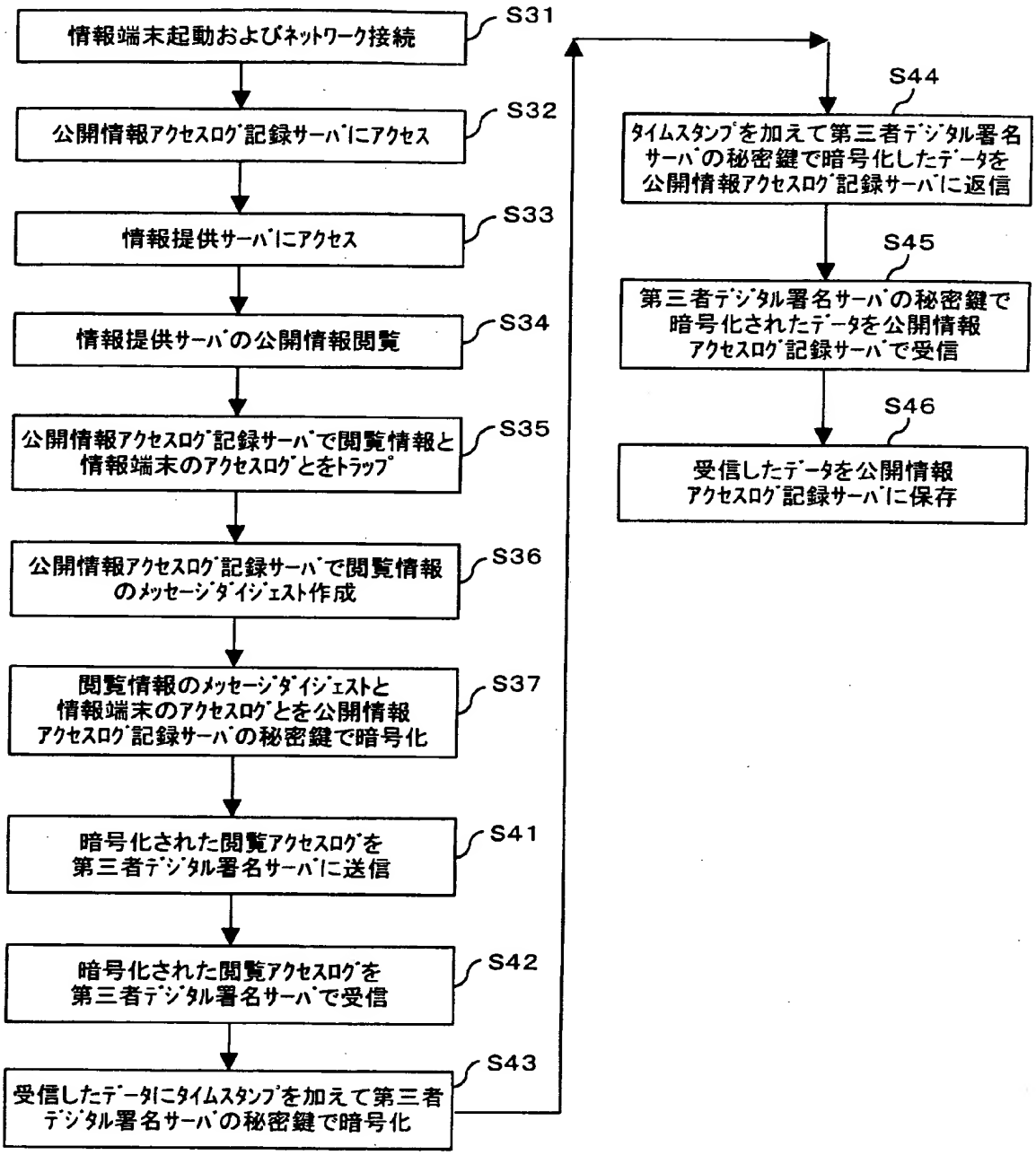
【図７】


情報端末起動およびネットワーク接続
S31
公開情報アクセスログ記録サーバにアクセス
S32
情報提供サーバにアクセス
S33
情報提供サーバの公開情報閲覧
S34
公開情報アクセスログ記録サーバで閲覧情報と情報端末のアクセスログとをトラップ
S35
公開情報アクセスログ記録サーバで閲覧情報のメッセージダイジェスト作成
S36
閲覧情報のメッセージダイジェストと情報端末のアクセスログとを公開情報アクセスログ記録サーバの秘密鍵で暗号化
S37
暗号化された閲覧情報のメッセージダイジェストとアクセスログとを公開情報アクセスログ記録サーバに保存
S38

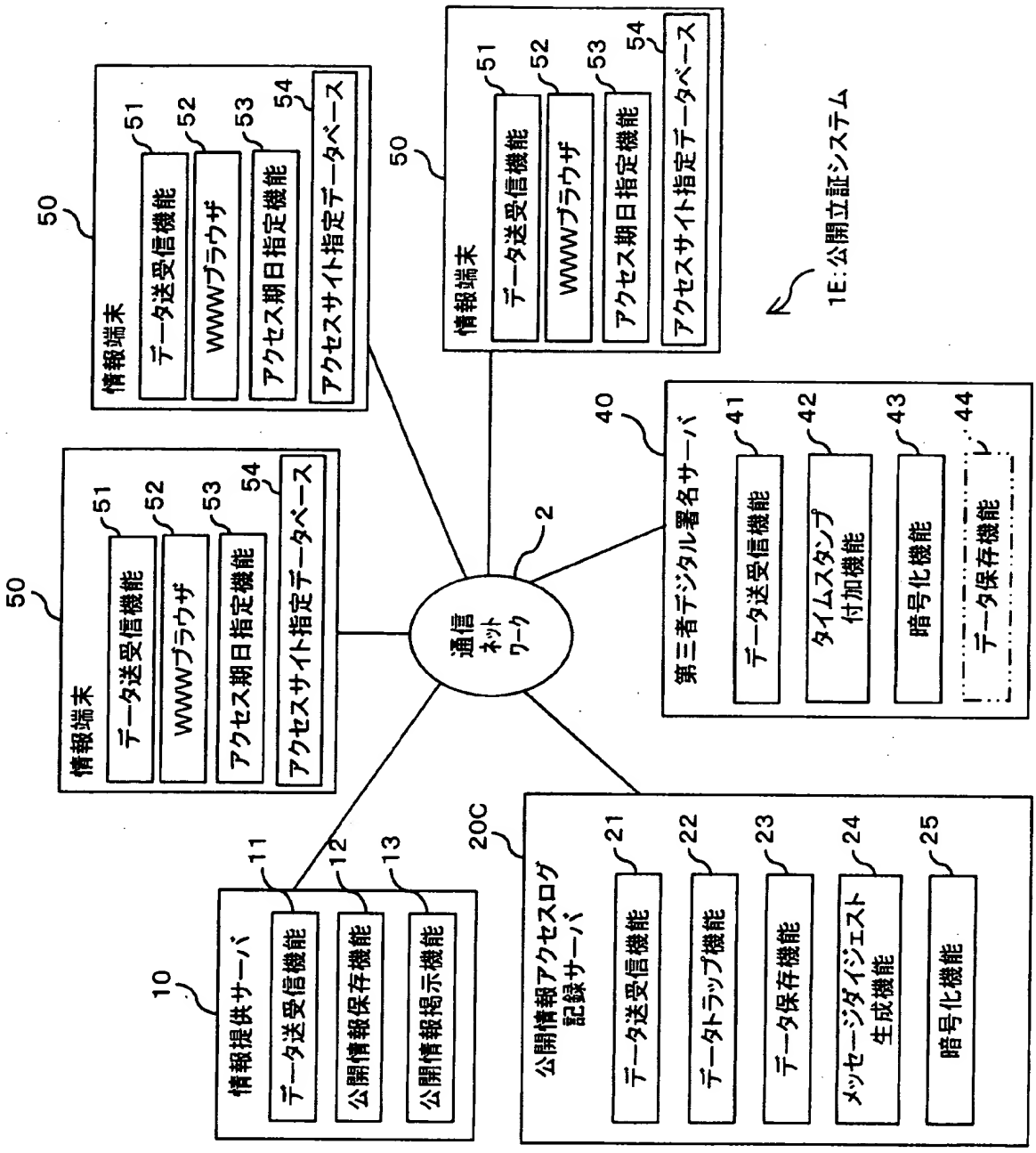
【図８】


1D:公開立証システム
10
情報提供サーバ
11
データ送受信機能
12
公開情報保存機能
13
公開情報掲示機能
2
通信ネットワーク
20C
公開情報アクセスログ記録サーバ
21
データ送受信機能
22
データトラップ機能
23
データ保存機能
24
メッセージダイジェスト生成機能
25
暗号化機能
30
情報端末
31
データ送受信機能
32
WWWブラウザ
40
第三者デジタル署名サーバ
41
データ送受信機能
42
タイムスタンプ付加機能
43
暗号化機能
44
データ保存機能

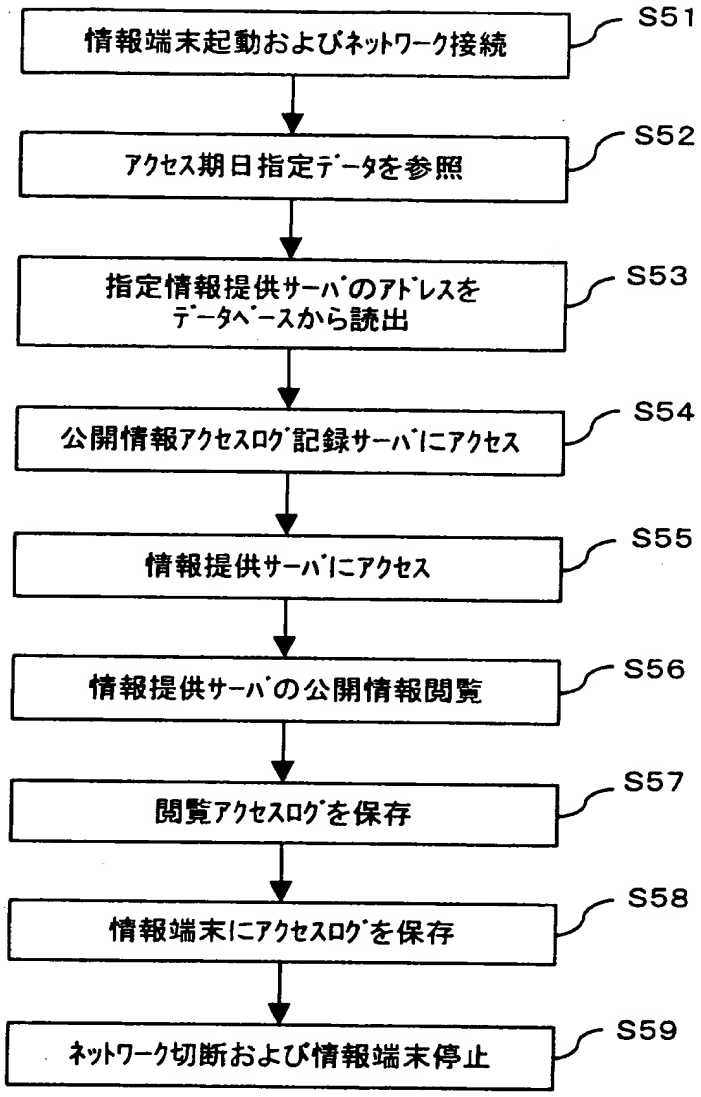
【図９】


情報端末起動およびネットワーク接続
S31
公開情報アクセスログ記録サーバにアクセス
S32
情報提供サーバにアクセス
S33
情報提供サーバの公開情報閲覧
S34
公開情報アクセスログ記録サーバで閲覧情報と情報端末のアクセスログとをトラップ
S35
公開情報アクセスログ記録サーバで閲覧情報のメッセージダイジェスト作成
S36
閲覧情報のメッセージダイジェストと情報端末のアクセスログとを公開情報アクセスログ記録サーバの秘密鍵で暗号化
S37
暗号化された閲覧アクセスログを第三者デジタル署名サーバに送信
S41
暗号化された閲覧アクセスログを第三者デジタル署名サーバで受信
S42
受信したデータにタイムスタンプを加えて第三者デジタル署名サーバの秘密鍵で暗号化
S43
タイムスタンプを加えて第三者デジタル署名サーバの秘密鍵で暗号化したデータを公開情報アクセスログ記録サーバに返信
S44
第三者デジタル署名サーバの秘密鍵で暗号化されたデータを公開情報アクセスログ記録サーバで受信
S45
受信したデータを公開情報アクセスログ記録サーバに保存
S46

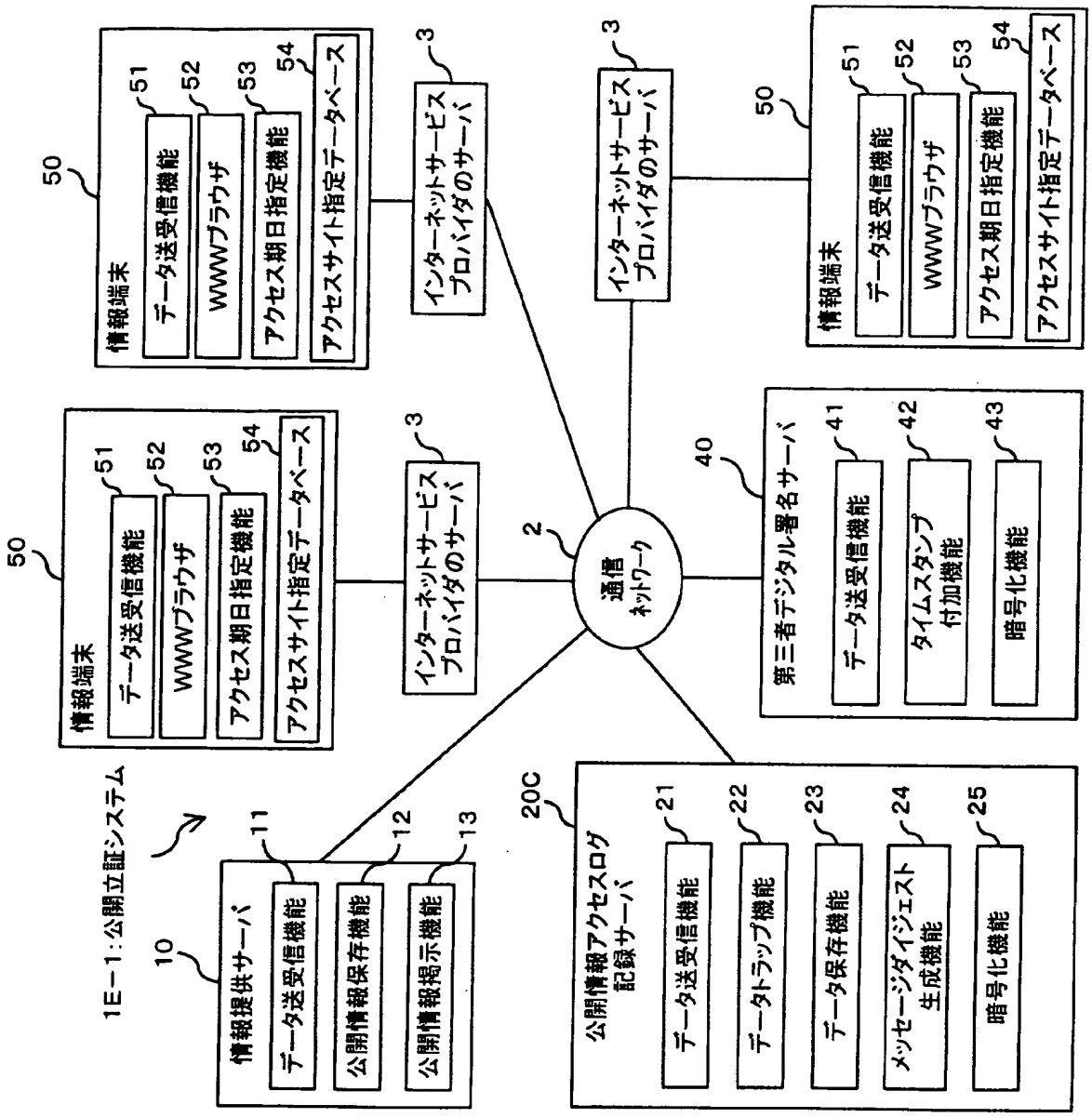
【図１０】


1E:公開立証システム
通信ネットワーク
2
情報提供サーバ
10
データ送受信機能
11
公開情報保存機能
12
公開情報掲示機能
13
公開情報アクセスログ記録サーバ
20C
データ送受信機能
21
データトラップ機能
22
データ保存機能
23
メッセージダイジェスト生成機能
24
暗号化機能
25
第三者デジタル署名サーバ
40
データ送受信機能
41
タイムスタンプ付加機能
42
暗号化機能
43
データ保存機能
44
情報端末
50
データ送受信機能
51
WWWブラウザ
52
アクセス期日指定機能
53
アクセスサイト指定データベース
54

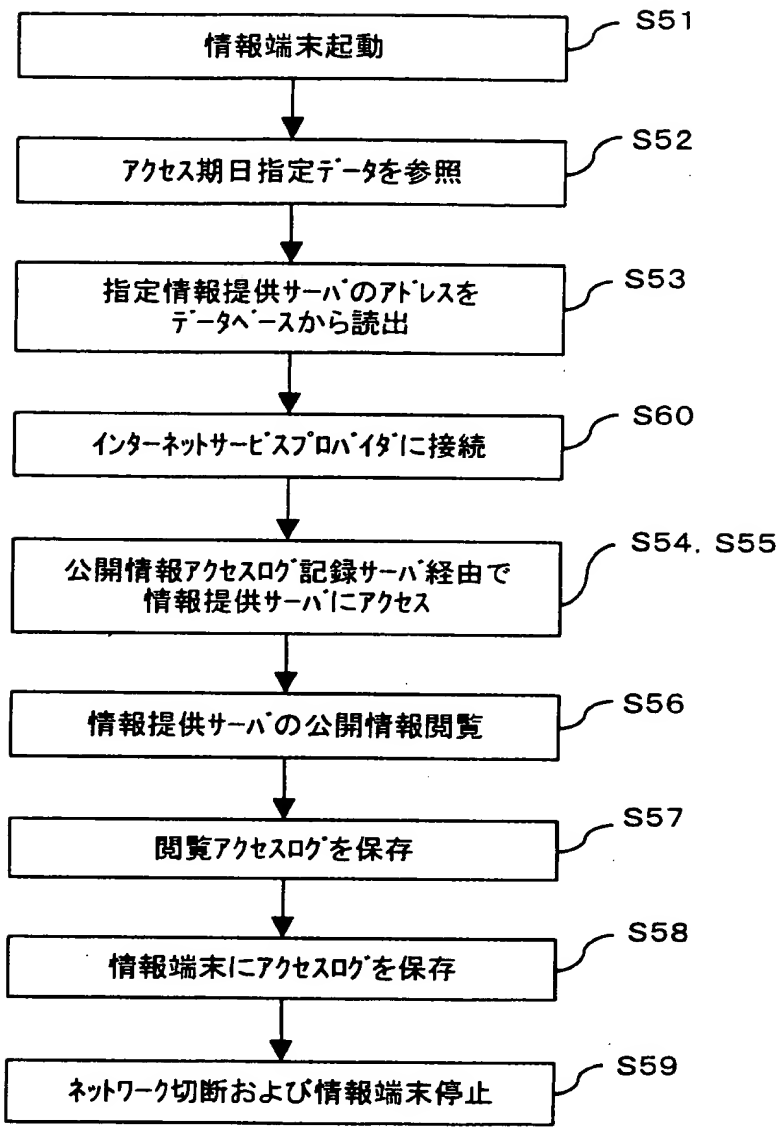
【図１１】


情報端末起動およびネットワーク接続
S51
アクセス期日指定データを参照
S52
指定情報提供サーバのアドレスを
データベースから読出
S53
公開情報アクセスログ記録サーバにアクセス
S54
情報提供サーバにアクセス
S55
情報提供サーバの公開情報閲覧
S56
閲覧アクセスログを保存
S57
情報端末にアクセスログを保存
S58
ネットワーク切断および情報端末停止
S59

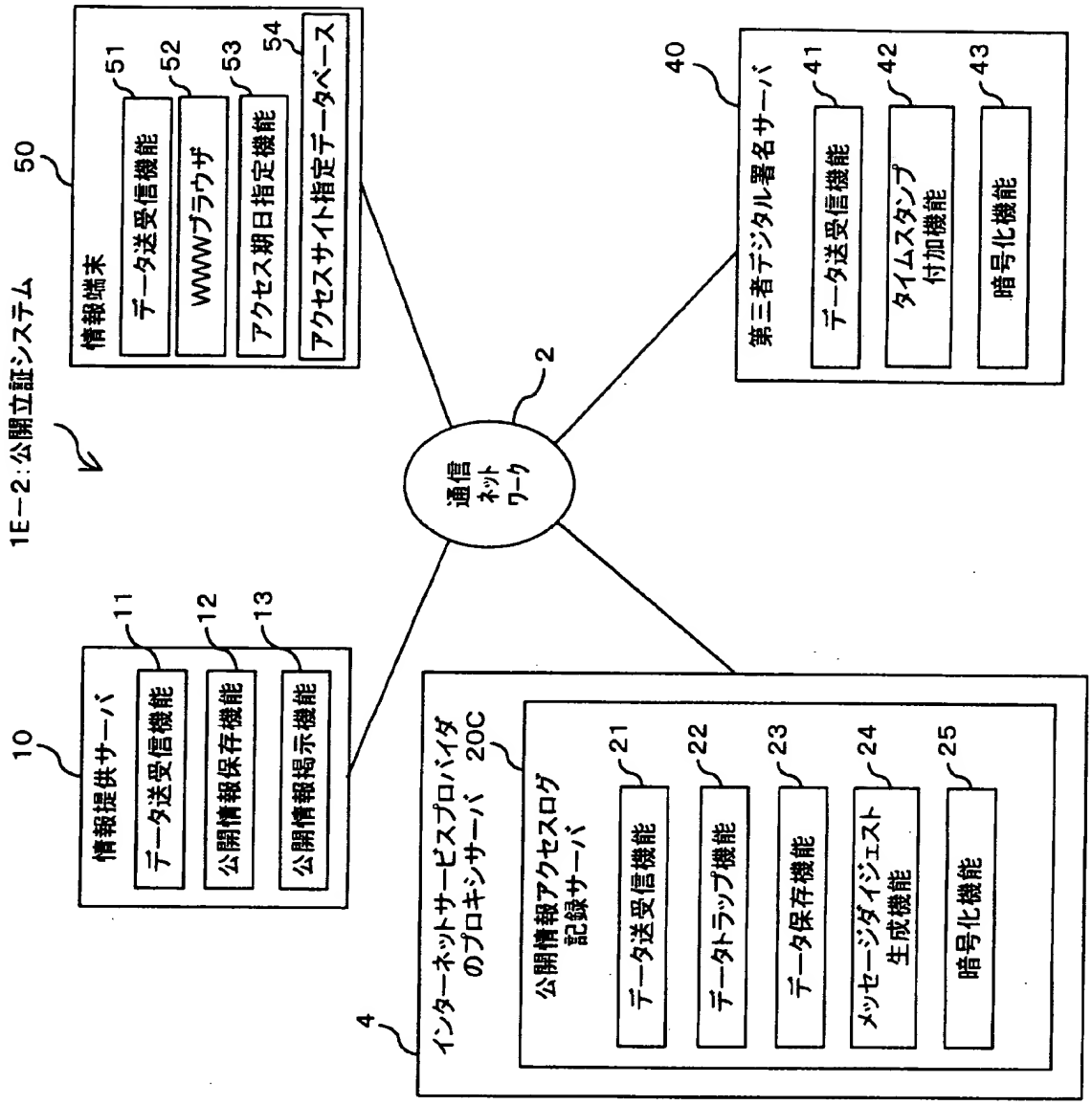
【図１２】


1E－1：公開立証システム
情報提供サーバ
10
データ送受信機能
11
公開情報保存機能
12
公開情報掲示機能
13
公開情報アクセスログ記録サーバ
20C
データ送受信機能
21
データトラップ機能
22
データ保存機能
23
メッセージダイジェスト生成機能
24
暗号化機能
25
通信ネットワーク
2
第三者デジタル署名サーバ
40
データ送受信機能
41
タイムスタンプ付加機能
42
暗号化機能
43
インターネットサービスプロバイダのサーバ
3
情報端末
50
データ送受信機能
51
WWWブラウザ
52
アクセス期日指定機能
53
アクセスサイト指定データベース
54

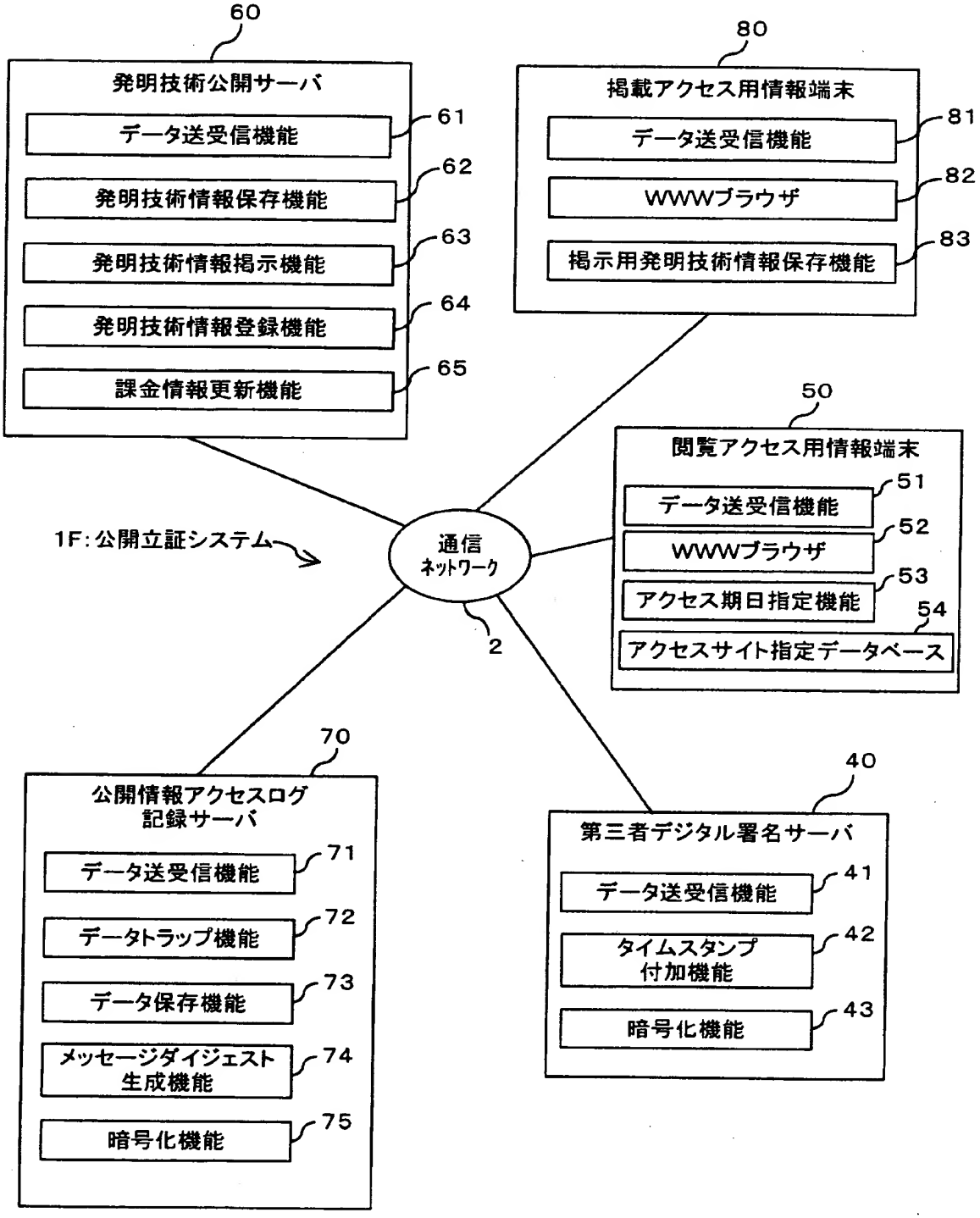
【図１３】


情報端末起動
S51
アクセス期日指定データを参照
S52
指定情報提供サーバのアドレスを
データベースから読出
S53
インターネットサービスプロバイダに接続
S60
公開情報アクセスログ記録サーバ経由で
情報提供サーバにアクセス
S54, S55
情報提供サーバの公開情報閲覧
S56
閲覧アクセスログを保存
S57
情報端末にアクセスログを保存
S58
ネットワーク切断および情報端末停止
S59

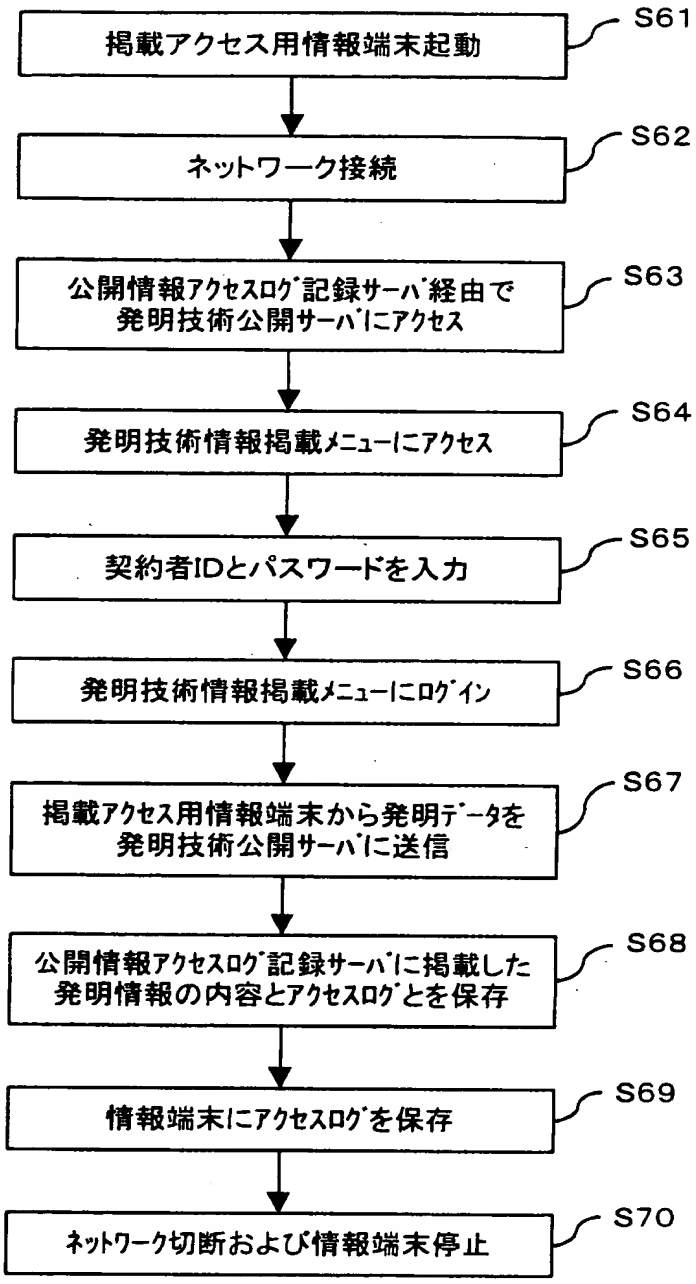
【図１４】


1E−2:公開立証システム
情報端末
50
データ送受信機能
51
WWWブラウザ
52
アクセス期日指定機能
53
アクセスサイト指定データベース
54
通信ネットワーク
2
第三者デジタル署名サーバ
40
データ送受信機能
41
タイムスタンプ付加機能
42
暗号化機能
43
情報提供サーバ
10
データ送受信機能
11
公開情報保存機能
12
公開情報掲示機能
13
インターネットサービスプロバイダのプロキシサーバ
20C
4
公開情報アクセスログ記録サーバ
データ送受信機能
21
データトラップ機能
22
データ保存機能
23
メッセージダイジェスト生成機能
24
暗号化機能
25

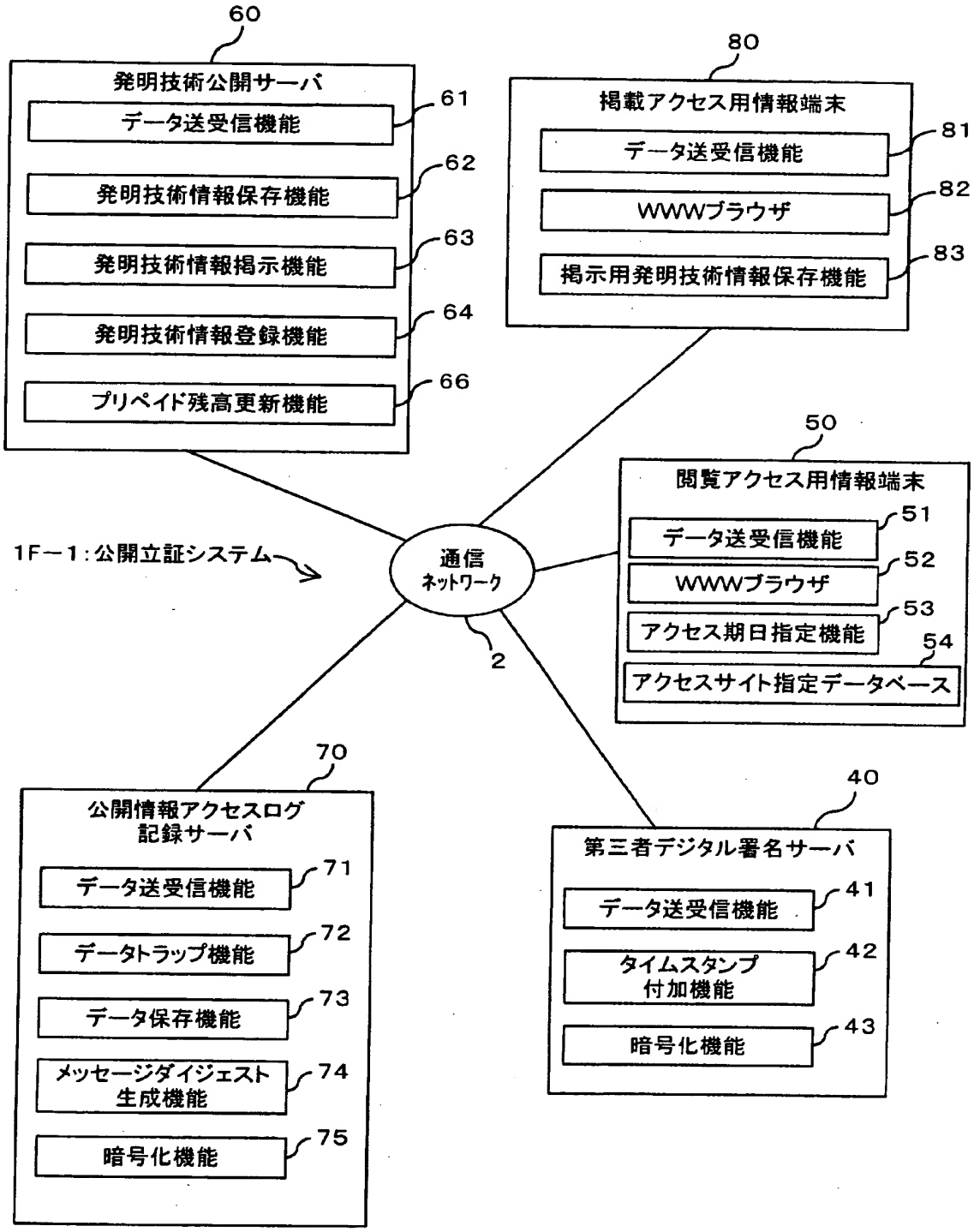
【図１５】


60
発明技術公開サーバ
データ送受信機能
61
発明技術情報保存機能
62
発明技術情報掲示機能
63
発明技術情報登録機能
64
課金情報更新機能
65
80
掲載アクセス用情報端末
データ送受信機能
81
WWWブラウザ
82
掲示用発明技術情報保存機能
83
50
閲覧アクセス用情報端末
データ送受信機能
51
WWWブラウザ
52
アクセス期日指定機能
53
54
アクセスサイト指定データベース
1F:公開立証システム
通信
ネットワーク
2
70
公開情報アクセスログ
記録サーバ
データ送受信機能
71
データトラップ機能
72
データ保存機能
73
メッセージダイジェスト
生成機能
74
暗号化機能
75
40
第三者デジタル署名サーバ
データ送受信機能
41
タイムスタンプ
付加機能
42
暗号化機能
43

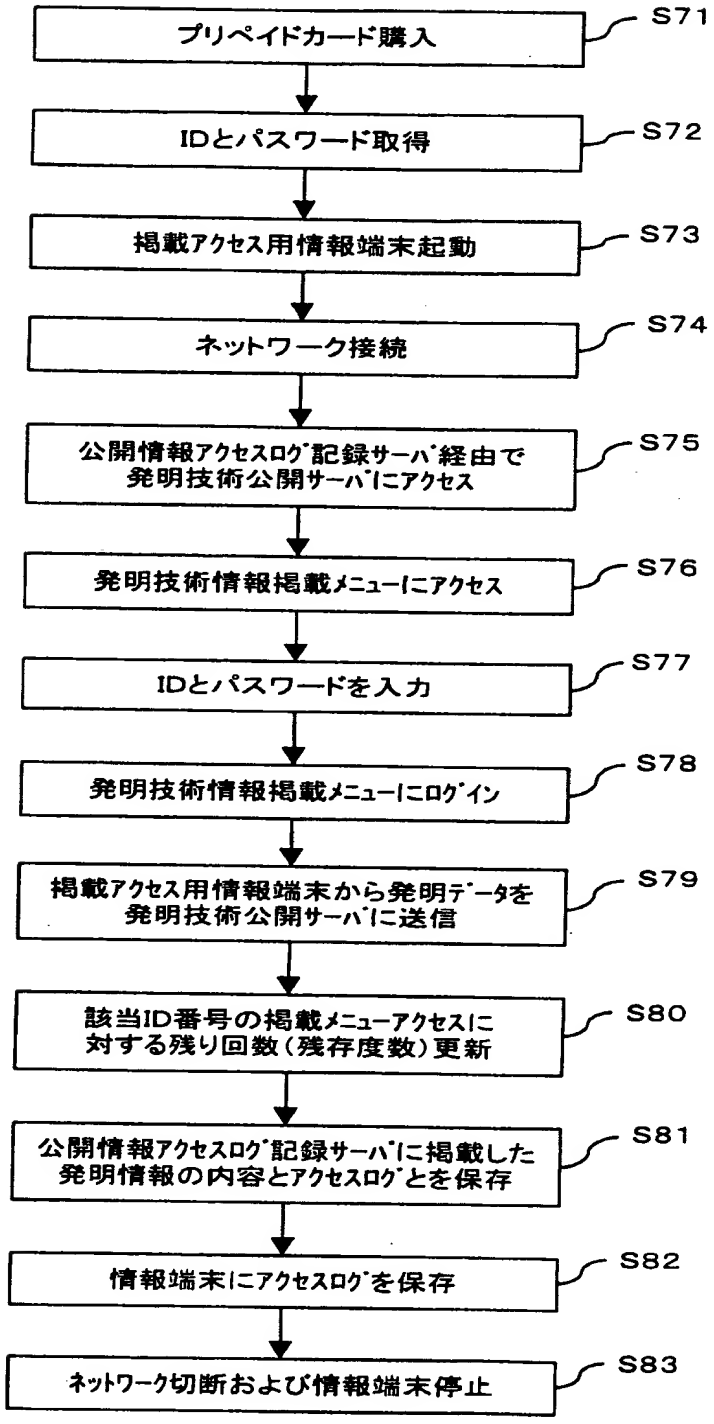
【図１６】


掲載アクセス用情報端末起動
S61
ネットワーク接続
S62
公開情報アクセスログ記録サーバ経由で
発明技術公開サーバにアクセス
S63
発明技術情報掲載メニューにアクセス
S64
契約者IDとパスワードを入力
S65
発明技術情報掲載メニューにログイン
S66
掲載アクセス用情報端末から発明データを
発明技術公開サーバに送信
S67
公開情報アクセスログ記録サーバに掲載した
発明情報の内容とアクセスログとを保存
S68
情報端末にアクセスログを保存
S69
ネットワーク切断および情報端末停止
S70

【図１７】


60
発明技術公開サーバ
データ送受信機能
61
発明技術情報保存機能
62
発明技術情報掲示機能
63
発明技術情報登録機能
64
プリペイド残高更新機能
66
80
掲載アクセス用情報端末
データ送受信機能
81
WWWブラウザ
82
掲示用発明技術情報保存機能
83
50
閲覧アクセス用情報端末
データ送受信機能
51
WWWブラウザ
52
アクセス期日指定機能
53
アクセスサイト指定データベース
54
1F－1：公開立証システム
通信
ネットワーク
2
70
公開情報アクセスログ
記録サーバ
データ送受信機能
71
データトラップ機能
72
データ保存機能
73
メッセージダイジェスト
生成機能
74
暗号化機能
75
40
第三者デジタル署名サーバ
データ送受信機能
41
タイムスタンプ
付加機能
42
暗号化機能
43

【図１８】


プリペイドカード購入
S71
IDとパスワード取得
S72
掲載アクセス用情報端末起動
S73
ネットワーク接続
S74
公開情報アクセスログ記録サーバ経由で
発明技術公開サーバにアクセス
S75
発明技術情報掲載メニューにアクセス
S76
IDとパスワードを入力
S77
発明技術情報掲載メニューにログイン
S78
掲載アクセス用情報端末から発明データを
発明技術公開サーバに送信
S79
該当ID番号の掲載メニューアクセスに
対する残り回数（残存度数）更新
S80
公開情報アクセスログ記録サーバに掲載した
発明情報の内容とアクセスログとを保存
S81
情報端末にアクセスログを保存
S82
ネットワーク切断および情報端末停止
S83

【書類名】　　要約書

【要約】

【課題】各種情報が電子データとしてネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データがネットワーク上で掲示・公開されていたことを立証できるようにして、そのネットワーク上で掲示・公開された情報にも、印刷物や出版物と同様の証拠能力をもたせることを実現する。

【解決手段】公開情報を保存する公開情報保存機能１２と、公開情報を閲覧すべく通信ネットワーク２を介してアクセスしてきた情報端末３０に対し公開情報を提供する公開情報掲示機能１３とを有する情報提供サーバ１０と、情報端末３０により閲覧された公開情報とこの公開情報に対するアクセス日時とを閲覧アクセスログとして獲得するデータトラップ機能２２と、このデータトラップ機能２２よって獲得された閲覧アクセスログを保存するデータ保存機能２３とを有する閲覧アクセスログ記録サーバ２０Ａとをそなえて構成する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社